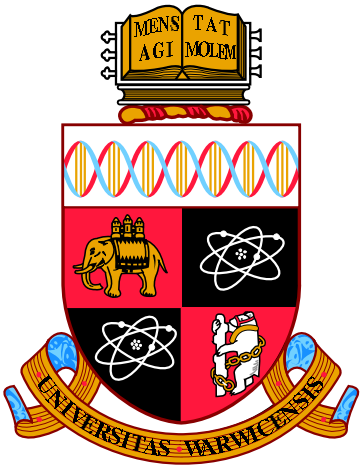


Perfect Powers that are Sums of Consecutive Like Powers

by

Vandita Patel

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

June 2017

Mathematics is the queen of the sciences and number theory is the queen of mathematics.

— *Carl Friedrich Gauss*

Contents

"Words fail me and tears flood to my eyes as I attempt to express my gratitude to and admiration for my legendary supervisor Samir Siksek, without whom I would still be at Canary Wharf fiddling with excel spreadsheets."

SS

Acknowledgments

My most sincere gratitude goes to my supervisor, Professor Samir Siksek, for initially inspiring me with the wonders of Number Theory, Diophantine equations and the p-adic world during my undergraduate years. Such was this inspiration that I could not bear to stay in the soul–less world of banking. Thank you for your guidance, patience, support and most importantly, brilliant sense of humour and giving me a second chance with mathemagics. 🪄

I am highly indebted to my collaborators, Professor Mike Bennett and Professor Samir Siksek, for introducing me to the work of Dr. Zhongfeng Zhang, which this thesis stems from. May we continue to have many fruitful collaborations!

With Samir and Mike in Turkey at one of my first conferences, during one of the excursions, I decided to chase The Peckin[1] up a hill; fascinated by its feathered feet. Thankfully, Samir came chasing after me, and just in time too. At the top of the hill was the farmer wielding his shotgun! Seriously, thank you for keeping me alive for four years, along with the support of many many friends and colleagues along the way. Not only in Turkey, but needing medical care in Sarajevo and Bordeaux (just to name a few - there are far too many instances of 'Van break-downs' to list). Special thanks must go to Samuele and Nicolas, for helping me to get off the plane when coming back to England for my defence - a memory that none of us will ever forget!

A special mention goes to Dr. Adam Harper, who thoroughly read a preliminary draft of this thesis (in the form of the infamous "Warwick Fourth Year Report") and his valuable suggestions helped to shape this thesis.

[1] A breed of chicken that walks like a penguin.
See a picture: www.photo-dictionary.com/phrase/11510/peckin.html

Special thanks goes to Dr. Piper Harron, for it was her original thesis that inspired me to inject all of my personality into mine.

A very special mention goes to Dr. Pieter Moree, for many helpful corrections to this thesis, but most importantly, for reminding me that mathemagics should be fun! 🪄

I would like to thank my examiners, Dr. Damiano Testa and Dr. Haluk Şengün for quite an enjoyable viva, for being super understanding during the viva and allowing me to sit on the floor, for their time in reading my work and for their many valuable improvements and corrections to this thesis.

To all of my supportive friends: Priya, Niketa, The Barclays Girls (Tasha, Sabrina, Luisa, Charlene, Alicia and Asena), Lyn, Chris W., Samuele, Heline, Céline, Kabs, Matt B., Milena, Mirna, Shu Ting, Peter K., Mike S., George T., George K., Mark B., Alejandro, Lilit and Alexandre - for their brilliant company, delicious teatimes (with waffles, crepes cakes and muffins, and the infamous mango cheesecake) and great humour.

I am much obliged to the Engineering and Physical Sciences Research Council (EPSRC), the Max Planck Institute for Mathematics in Bonn and the Warwick Mathematics Institute for their financial support during my time as a PhD student. I extend my gratitude to the friendly staff (especially to Carole and Rimi at Warwick and Cerolein and Svenja at MPI), PhD students and the Number Theory group at both institutions.

Ultimately, this thesis would not have been written without the love, encouragement and moral support of my family. To my mother, Priti, and brother, Dipesh, for their unconditional love. To my dearest Pravin; for always listening to my muddled mathematical thoughts, for making many cups of tea precisely at the moments when they are most needed, for the random spontaneous hugs and kisses and unlimited love.

This thesis was typeset with LaTeX 2_ε[2] by the author.

[2] LaTeX 2_ε is an extension of LaTeX. LaTeX is a collection of macros for TeX. TeX is a trademark of the American Mathematical Society. The style package *warwickthesis* was used.

Declarations

The results presented in Parts I and II are, to the best of the author's knowledge, entirely new, unless otherwise stated. Many of these results have now been accepted for publication (see Bennett et al. [2017] and Patel and Siksek [2017]).

Part I is based on collaborative work with Professor Michael A. Bennett (University of British Columbia, Vancouver, Canada) and Professor Samir Siksek (University of Warwick, England), which has now been published (see Bennett et al. [2017]).

Part II is based on collaborative work with Professor Samir Siksek (University of Warwick, England), which has also been published (see Patel and Siksek [2017]).

Abstract

This thesis is concerned with finding integer solutions to certain Diophantine equations. In doing so, we will use a variety of techniques. Unfortunately, we are not able to mention all of them - there are many techniques in solving Diophantine equations! Combining analytic methods with classic and modern algebraic approaches proves fruitful in a number of cases.

Our focus will be on the following Diophantine equation:

$$(x+1)^k + \cdots + (x+d)^k = y^n, \quad x,\ y,\ n,\ d,\ k \in \mathbb{Z}, \quad d,\ k,\ n \geq 2, \qquad (\clubsuit)$$

For fixed integers d and k, we would like to determine all of the integer solutions (x, y, n).

Euler noted the relation $6^3 = 3^3 + 4^3 + 5^3$ and asked for other instances of cubes that are sums of consecutive cubes. Similar problems have been studied by Cunningham, Catalan, Genocchi, Lucas and Pagliani.

Using only elementary arguments, Cassels [1985] and Uchiyama [1979] independently solved equation ($\clubsuit$) in the case $k = d = 3$ and $n = 2$.

Stroeker [1995] considered equation ($\clubsuit$) in the case $k = 3$, $2 \leq d \leq 50$ with $n = 2$. He determined all squares that can be written as a sum of at most 50 consecutive cubes.

Zhang [2014] solved equation ($\clubsuit$) for $k \in \{2, 3, 4\}$, $d = 3$ and $n \geq 2$ using Frey–Hellegouarch curves and the modular method. These two considerations play a key role in this thesis.

In Part I of this thesis, we generalise Stroeker's and Zhang's work by determining all perfect powers that are sums of at most 50 consecutive cubes (see Bennett et al. [2017]). We solve equation (♣) in the case $k = 3$, $2 \leq d \leq 50$ and $n \geq 2$. Here is an example of a sum of 49 consecutive cubes that is again a cube:

$$291^3 + 292^3 + 293^3 + 294^3 + ... + 337^3 + 338^3 + 339^3 = 1155^3.$$

Our methods include: descent, linear forms in two logarithms, sieving and Frey-Hellegouarch curves.

In Part II of this thesis, we let $k \geq 2$ be an even integer and r a non-zero integer. We show that for almost all $d \geq 2$ (in the sense of natural density), the equation

$$x^k + (x + r)^k + \cdots + (x + (d - 1)r)^k = y^n, \qquad x,\ y,\ n \in \mathbb{Z}, \qquad n \geq 2,$$

has no solutions (see Patel and Siksek [2017]). The techniques employed here are vastly different to those used in Part I. We move away from solving individual equations and instead present a result which shows the general behaviour of these equations. Our main considerations are the Bernoulli polynomials, their 2-adic Newton polygons and their Galois groups.

"What day is it?" asked Pooh.
"It's today" squeaked Piglet.
"My favourite day", said Pooh.

Winnie the Pooh, A. A. Milne

Chapter 1

Diophantine Equations

Our journey begins in Ancient Greece, where Diophantus of Alexandria is erratically writing his series of Arithmetica. Little does he know at this stage that his collective works will become infamous. Our mysterious Diophantus is compiling problems and in some instances, even providing the solutions! He wants to find all integer solutions to certain algebraic equations. Problems such as these are nowadays called *Diophantine equations*, named aptly after him. Typically, Diophantine equations have integer coefficients and we seek only integer solutions.

Information and insight into the life of Diophantus is sparse. Our alluding mathematician is believed to have existed around 201–299 AD. Within his mathematical puzzles and riddles, he did leave behind clues to decipher his age[1]:

'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:
'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
After attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years, he ended his life.'

[1]Rumour has it that Metrodorus collected such mathematical epigrams and wrote very few of them. Perhaps Diophantus himself wrote this particular riddle, in which case this cannot be his true final age. Unfortunately, there are no current sources available to verify the age of Diophantus and I am afraid that I will have to leave you in suspense.

[1]The solution to this problem does not exist anywhere in this thesis (page numbers do not count).

Many of the books in the series *Arithmetica* have been lost or destroyed and only a few managed to survive. Pierre de Fermat (1601–1665 AD) was a French jurist who extensively studied the works of Diophantus, often daydreaming about Diophantine equations during trials. He was obsessed. He is notably famous for writing in the margin of the 1621 edition of Arithmetica (written by Bachet):

"If an integer n is greater than 2, then $a^n + b^n = c^n$ has no solutions in non-zero integers a, b, and c. I have a truly marvelous proof of this proposition which this margin is too narrow to contain."

Crowned *Fermat's Last Theorem* despite not being even close to a theorem (this was a conjecture at the time since Fermat had not *actually* provided a proof), Fermat's missing proof eluded amateur and professional mathematicians alike for over 350 years!

Fermat's Infinite Descent

Fermat himself proved that there are no integer solutions when $n = 3$ or $n = 4$ (as did Euler independently but much later) using a very clever trick: Fermat's method of *infinite descent*. Using an elementary factorisation argument, Fermat showed that if there is a solution then there also exists a smaller solution. Thus if we start out with a minimal solution then we obtain a contradiction.

The case $n = 5$

Dirichlet (1828) and Legendre (1830) provided a proof for the case $n = 5$. Legendre's method of proof is attributed to Marie–Sophie Germain, who was unjustly mentioned *only* in the footnote!

The work of amateur mathematician, Sophie Germain, provided the first major breakthrough in the history of the Fermat equation. With a single theorem, she was able to solve the Fermat equation for *many* values of n. Previously, many other mathematicians had contributed to the effort with solutions for *only* individual values of n; Stewart and Tall [2016] contains an extensive history.

Sophie Germain: Rebel Mathematician

Confined to her Parisian home during the Great French Revolution (1789–1794 AD), a young Sophie took a keen interest in the books in her father's library. There, she discovered wonders within J. E. Montucla's *L'Histoire des Mathématiques*. Reading about the death of Archimedes (Roman forces had captured the city, and legend says that Archimedes ignored commands from a Roman soldier, claiming that he was far too engrossed in his mathematical diagrams - leading to his sudden death-by-sword), she reaches the conclusion: if geometry is so captivating as to lead to death, then it is the only thing worth living for.

Her sudden desire to pursue the mathematical sciences was immediately met with resistance, both from family and friends as well as society. Her parents were concerned with her "abnormal" behaviour, punishing her even. Yet young Sophie was undeterred and she would often work late into the night. Her parents would confiscate her candles, clothing and even heating to deter her. Despite this, Sophie continued to work on mathematics, wrapping herself in bed linen and writing deep into the night while the ink slowly froze in it's well.

In 1794, L'École Polytechnique opened in Paris, a perfect place for Sophie to study mathematics further. However, one caveat existed: the institute did not admit women. Taking on the identity of a former student who had left Paris, Sophie managed to enrol at the college. She continued to take on this identity for most of her career, including all correspondences between herself and prominent mathematicians of the time.

Writing under the alias of "Auguste Antoine LeBlanc" she provided a proof to Fermat's Last Theorem, (under the assumption that n does not divide a, b or c) for all values of $n \leq 100$. Actually, her methods were readily applicable to all $n \leq 197$. For at least a century after Germain, mathematicians were adapting her methods to reach contradictions for the Fermat equation for very large values of n. Here are a few of the milestones reached in the history of the Fermat equation.

- 1823 – S. Germain; $n \leq 100$ and $n \leq 197$.
- 1908 – L. E. Dickson; $n \leq 7,000$.
- 1976 – S. S. Wagstaff; $n \leq 125,000$.
- 1988 – A. Granville and M. Monagan; $n \leq 714,591,416,091,389$.

In Part I, Chapter 7, we will revisit and adapt Germain's method to arrive at contradictions for the majority of our equations.

Bounding n

We now have the possibility of solving Fermat's Last Theorem for individual values of n, perhaps a new strategy would be to find an upper bound for n, thus leaving us with a manageable finite computation. Bounding the exponent n, or bounding any variable in our Diophantine equation lies at the foundation of the pioneering work of *Alan Baker*, Fields Medal winner for developing the area *Linear Forms in Logarithms*. This technique gives *effective* bounds for unknowns in certain Diophantine equations. Unfortunately Baker's theory is inapplicable to the Fermat equation.

When Baker's theory is applicable, it usually produces colossal bounds. The question of interest has now changed: do we have computational power to carry out the *finite* computation?

In Part I, Chapter 3, we explore Baker's method and a direct application to our equations show very clearly how large these bounds can be. In Part I, Chapter 6, refinements of Baker's method for linear forms in *two* logarithms, given by Laurent [2008] yield more manageable bounds for n.

Proof of Fermat's Last Theorem: There are no non-trivial solutions!

The proof to the elusive Fermat's Last Theorem came in 1995, when Wiles announced his complete proof. The argument did not build on any of the previous work and attempts that I have outlined above. A completely different approach was used, and the story for this work begins in 1975, when Yves Hellegouarch associated *Elliptic curves* to equations like $a^n + b^n = c^n$. His focus was not on the Fermat conjecture and it was only in 1982 that Gerhard Frey made the connection between this curve and the Fermat equation. Frey noticed that the curve constructed (and its mod p representation) has some very special properties. Soon thereafter, Serre formulated a precise conjecture which implies Fermat's Last Theorem. Ribet [1990] proved enough of this conjecture to show that Fermat's Last Theorem follows from the famous *Taniyama–Shimura conjecture*. The Taniyama–Shimura conjecture (also called the modularity conjecture) was proved by Wiles [1995] for semistable elliptic curves, which was enough to prove Fermat's Last Theorem. This circle of ideas gave rise to the *modular method* for attacking Diophantine equations, which will be crucial for us in Chapter 8.

Algorithm to Solve all Diophantine Equations?

The methods used by Diophantus to solve algebraic equations are somewhat ad-hoc. One may be able to work through 100 of his problems, yet will not be able to use the methods developed to solve the next problem. In this introduction, we have listed many different approaches to studying Diophantine equations, but I believe that we have barely scratched the surface - there are many more methods which I have not included in my exposition! This leads us to question whether it is possible to find a uniform method to determine all of the solutions to any algebraic equation, preferably a method that terminates in a finite number of steps (called an *algorithm*)? This was indeed the essence of *Hilbert's tenth problem*, which states:

"Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable

in rational integers."

In 1970, Yuri Matiyasevich answered Hilbert's question in the negative: no such algorithm can exist. However, there is hope to find algorithms, or structured methods to solve large families of Diophantine equations - this notion is explored in Part I of this thesis.

Given that one single sole method does not exist makes research in Diophantine equations remarkably alluring, bewitching, captivating, dazzling and exhilarating (and rather frustrating[2] at times too!) for both mathematicians and non-mathematicians. There is always room and scope for the development of new methods and techniques!

1.1 This Thesis - Structure and Navigation

This thesis is organised in two parts, each with its own self-contained introduction that also contains a detailed review of the literature. Part I, uses a variety methods in solving Diophantine equations to answer the question: when is a sum of at most 50 consecutive cubes a perfect power? Part II looks at the question: when is a sum of d consecutive powers a perfect power. The flavour and style of mathematics is vastly different to that in Part I. We move away from solving individual equations and instead, provide rigour to the notion that when one is looking for integer solutions where the exponents of the consecutive integers are even, solutions are rare.

Part I

We consider the equation

$$(x+1)^3 + (x+2)^3 + \cdots + (x+d)^3 = y^\ell \qquad x,\ y,\ \ell,\ d \in \mathbb{Z}, \qquad \ell \geq 2 \qquad (1.1)$$

and we are interested in finding all integer solutions (x, y, ℓ) when $2 \leq d \leq 50$. We can work under the assumption that ℓ is prime, and are able to recover solutions for any integer ℓ from our table of solutions which shows solutions for prime[3] values of ℓ. We recover the solutions of Stroeker [1995] when $\ell = 2$. Surprisingly, we also unearth five brand new non-trivial solutions when $\ell = 3$, as well as recovering the

[2]The A–B–C–D–E–F of Diophantine Equations. Notice the imbalance in feelings?

[3]There are no further solutions for composite values of ℓ in our table, which only shows solutions when $x \geq 1$. However, solutions with composite ℓ do appear when considering any integer value x, for example $1^3 + 2^3 + \cdots + 8^3 = 36^2 = 6^4$. We explain how to obtain solutions for any value of x from our tables in Chapter 2.

solution of Euler, $3^3+4^3+5^3=6^3$. This part of the thesis is based on the published work Bennett et al. [2017].

In order to find all of the integer solutions, we first obtain an upper bound for our exponent ℓ. This leaves us with a finite number of equations, whereby we begin the process of discarding equations when they do not have a solution. Once we are left with a handful of equations, we can then determine all of the solutions.

Table 1.1 outlines the methodology used to discard equations, with a count for the number of equations remaining to be solved. We include references for the relevant chapters of Part I, so if you are interested in a particular methodology, then this has been hyperlinked for fast access (I know how eager everyone is to start solving 200 million equations - see Chapter 7)!

Chapter	Methods used to Solve Equation (1.1)	Number of Equations to Solve
2	Useful equations and identities	49 equations in (x, y, ℓ)
3	$\ell = 2$: Integer points on elliptic curves	49 equations in (x, y)
4	$d = 2$: Results of Nagell	2 equations in (x, y, ℓ)
5	First descent: a factorisation for $\ell \geq 5$	906 equations in (x, y, ℓ)
6	Linear Forms in two logarithms: $\ell \geq 5$ Bounding $\ell < 3 \times 10^6$	$906 \times 216814 = 196,433,484$ equations in (x, y)
7	Sophie-Germain type criterion (case $r \neq t$) $879 \times 216814 = 190,579,506$ in (x, y)	224 remain in (x, y)
8	Modularity[4] (case $r = t$) $27 \times 216814 = 5,853,978$ in (x, y)	53 remain in (x, y)
5.3	First descent when $\ell = 3$	942 equations in (x, y)
	Equations remaining via 5.3, 7 and 8	1219 remain in (x, y)
9.1	Local solubility tests	507 remain in (x, y)
9.2	A further descent	226 remain in (x, y)
10	Thue solver!	6 solutions found!

Table 1.1: Tracking the Number of Equations to Solve

[4]We put 27 out of the 906 equations through the modular method. In theory, we could put all 906 equations through the modular method, thus using modularity to bound ℓ and therefore not needing Chapters 6 and 7. This would be computationally very expensive and a waste of resources. Plus, the linear forms in logarithms and criterion adapted from Sophie Germain give rise to some incredibly beautiful mathemagics 🪄 which we would not want the reader to miss out on!

Part II

We study the equation:

$$x^k + (x+r)^k + \cdots + (x+(d-1)r)^k = y^n, \qquad x,\ y,\ n \in \mathbb{Z}, \qquad n \geq 2 \qquad (1.2)$$

and we give density results for the solutions of this equation when k is any positive even integer. Loosely speaking, we show that if you were to choose a value of d from the natural numbers at random, then there is 100% chance that the equation has no integer solutions. In Part II, we provide rigour to this notion, along with the relevant background material. This part of the thesis is based on the published work Patel and Siksek [2017].

Disclaimer: Don't worry if terms appear(ed) that are not immediately understandable in introductory sections - I will try to give a high level overview of these concepts without assuming too much background knowledge within the *Background* sections of each subsequent chapter. If the terms are completely comprehensible, then please feel free to omit the *Background* sections.

Part I

Perfect Powers that are Sums of Consecutive Cubes

— When shall we three meet again?
In thunder, lightning, or in rain?
— When the hurlyburly's done,
when the battle's lost and won.

Shakespeare, Macbeth

Chapter 2

Introduction

Euler, in his 1770 *Vollständige Anleitung zur Algebra* [Euler, 1770, art. 249], notes the relation

$$6^3 = 3^3 + 4^3 + 5^3, \tag{2.1}$$

and asks for other instances of cubes that are sums of three consecutive cubes. Dickson's *History of the Theory of Numbers* gives an extensive survey of early work on the problem of cubes that are sums of consecutive cubes [Dickson, 1971, pp. 582–585], and also squares that are sums of consecutive cubes [Dickson, 1971, pp. 585–588] with contributions by illustrious names such as Cunningham, Catalan, Genocchi and Lucas. Both problems possess some parametric families of solutions; one such family was constructed by Pagliani [1829/30]:

$$\left(\frac{v^5 + v^3 - 2v}{6}\right)^3 = \sum_{i=1}^{v^3} \left(\frac{v^4 - 3v^3 - 2v^2 - 2}{6} + i\right)^3, \tag{2.2}$$

where the congruence restriction $v \equiv 2$ or $4 \mod 6$ ensures integrality of the cubes. Pagliani constructed this paramteric family in response to a challenge (posed in the same journal) of giving 1000 consecutive cubes whose sum is a cube. Of course, the problem of squares that are sums of consecutive cubes possesses the well-known parametric family of solutions

$$\left(\frac{d(d+1)}{2}\right)^2 = \sum_{i=1}^{d} i^3 = \sum_{i=0}^{d} i^3.$$

These questions have continued to be of intermittent interest throughout a period of over 200 years. For example, Lucas states incorrectly in [Lucas, 1961, page 92]

that the only square expressible as a sum of three consecutive positive cubes is

$$6^2 = 1^3 + 2^3 + 3^3. \tag{2.3}$$

Independently, both Cassels [1985] and Uchiyama [1979] determine the squares that can be written as sums of three consecutive cubes (without reference to Lucas) showing that the only solutions in addition to (2.3) are

$$0 = (-1)^3 + 0^3 + 1^3, \qquad 3^2 = 0^3 + 1^3 + 2^3, \qquad 204^2 = 23^3 + 24^3 + 25^3. \tag{2.4}$$

Lucas also states that the only square that is the sum of two consecutive positive cubes is $3^2 = 1^3+2^3$ and the only squares that are sums of 5 consecutive non-negative cubes are

$$10^2 = 0^3 + 1^3 + 2^3 + 3^3 + 4^3, \qquad 15^2 = 1^3 + 2^3 + 3^3 + 4^3 + 5^3,$$
$$315^2 = 25^3 + 26^3 + 27^3 + 28^3 + 29^3, \qquad 2170^2 = 96^3 + 97^3 + 98^3 + 99^3 + 100^3,$$
$$2940^2 = 118^3 + 119^3 + 120^3 + 121^3 + 122^3.$$

These two claims turn out to be correct as shown by Stroeker [1995]. In modern language, the problem of which squares are expressible as the sum of d consecutive cubes, reduces for any given $d \geq 2$, to the determination of integral points on a genus 1 curve. Stroeker [1995], using a (by now) standard method based on linear forms in elliptic logarithms, solves this problem for $2 \leq d \leq 50$.

The problem of expressing arbitrary perfect powers as a sum of d consecutive cubes with d small has received somewhat less attention, likely due to the fact that techniques for resolving such questions are of a much more recent vintage. Zhongfeng Zhang [2014] showed that the only perfect powers that are sums of three consecutive cubes are precisely those already noted by Euler (2.1), Lucas (2.3) and Cassels (2.4). Zhang's approach is to write the problem as

$$y^n = (x-1)^3 + x^3 + (x+1)^3 = 3x(x^2+2), \tag{2.5}$$

and apply a descent argument that reduces this to certain ternary equations that have already been solved in the literature.

We develop a structured approach to this problem, determining all perfect powers that are sums of at most 50 cubes. Here is an example of a sum of 49

consecutive cubes that is again a cube:

$$291^3 + 292^3 + 293^3 + 294^3 + \cdots + 337^3 + 338^3 + 339^3 = 1155^3.$$

We easily verify that this solution (or indeed any of the other solution for $\ell = 3$ that is not Lucas' identity) does not belong to Pagliani's family simply by checking that the equation (or amended equation)

$$\frac{v^5 + v^3 - 2v}{6} = 1155$$

has no rational solutions.

2.1 The Results

In this part of this thesis, we consider the equation

$$(x+1)^3 + (x+2)^3 + \cdots + (x+d)^3 = y^\ell, \quad x,\ y,\ \ell,\ d \in \mathbb{Z}, \quad d,\ \ell \geq 2.$$

We extend the work of Stroeker [1995] and determine all perfect powers that are sums of d consecutive cubes, with $2 \leq d \leq 50$. This upper bound is somewhat arbitrary as our techniques extend to essentially any fixed values of d. In addition to Stroeker's solutions for $\ell = 2$ and Euler's solution for $\ell = 3$ (2.1), we find the following 5 additional solutions, all corresponding to the value $\ell = 3$.

$$\begin{gathered}
11^3 + 12^3 + 13^3 + 14^3 = 20^3, \\
3^3 + 4^3 + 5^3 + \cdots + 22^3 = 40^3, \\
15^3 + 16^3 + 17^3 + \cdots + 34^3 = 70^3, \\
6^3 + 7^3 + 8^3 + \cdots + 30^3 = 60^3, \\
291^3 + 292^3 + 293^3 + \cdots + 339^3 = 1155^3.
\end{gathered}$$

Remark: The additional solutions found for $\ell = 3$ stated above cannot be derived from Pagliani's parametric family of solutions (see equation (2.2)). Euler's solution is part of Pagliani's parametric family: in equation (2.2), let $v = 2$.

In this part of the thesis, we prove the following theorem. We expand upon the published joint paper Bennett et al. [2017] and give a full exposition.

Theorem 2.1.1. *Let $2 \leq d \leq 50$. Let ℓ be a prime. The integral solutions (x, y, ℓ)*

to the equation

$$(x+1)^3 + (x+2)^3 + \cdots + (x+d)^3 = y^\ell \tag{2.6}$$

with $x \geq 1$ *are given in Table 2.1.*

Table 2.1: The solutions to equation (2.6) with $2 \leq d \leq 50$, ℓ prime and $x \geq 1$.

d	(x, y, ℓ)
2	
3	(22, ± 204, 2), (2,6,3)
4	(10,20,3)
5	(24, ± 315, 2), (95, ± 2170, 2), (117, ± 2940, 2)
6	
7	(332, ± 16296, 2)
8	(27, ± 504, 2)
9	(715, ± 57960, 2)
10	
11	(1314, ± 159060, 2)
12	(13, ± 312, 2)
13	(143, ± 6630, 2), (2177, ± 368004, 2)
14	
15	(24, ± 720, 2), (3352, ± 754320, 2), (57959, ± 54052635, 2)
16	
17	(8, ± 323, 2), (119, ± 5984, 2), (4887, ± 1412496, 2)
18	(152, ± 8721, 2), (679, ± 76653, 2)
19	(6830, ± 2465820, 2)
20	(2,40,3), (14,70,3)
21	(13, ± 588, 2), (143, ± 8778, 2), (9229, ± 4070220, 2)
22	
23	(12132, ± 6418104, 2)
24	
25	(15587, ± 9742200, 2), (5,60,3)
26	
27	(19642, ± 14319396, 2)
28	(80, ± 4914, 2)
29	(24345, ± 20474580, 2)

Continued on next page

Table 2.1 – continued from previous page

d	(x, y, ℓ)
30	
31	(29744, ± 28584480, 2)
32	(68, ± 4472, 2), (132, ± 10296, 2), (495, ± 65472, 2)
33	(32, ± 2079, 2), (35887, ± 39081504, 2)
34	
35	(224, ± 22330, 2), (42822, ± 52457580, 2)
36	
37	(50597, ± 69267996, 2)
38	
39	(110, ± 9360, 2), (59260, ± 90135240, 2)
40	(3275, ± 1196520, 2)
41	(68859, ± 115752840, 2)
42	(63, ± 5187, 2)
43	(79442, ± 146889204, 2)
44	
45	(175, ± 18810, 2), (91057, ± 184391460, 2)
46	
47	(103752, ± 229189296, 2)
48	(63, ± 5880, 2), (409, ± 62628, 2), (19880, ± 19455744, 2), (60039, ± 101985072, 2)
49	(117575, ± 282298800, 2), (290,1155,3)
50	(1224, ± 312375, 2)

2.2 Without Loss of Generality, let $x \geq 1$

The restriction $x \geq 1$ imposed in the statement of Theorem 2.1.1 is merely to exclude a multitude of artificial solutions. Solutions with $x \leq 0$ can in fact be deduced easily, as we now explain:

(i) The value $x = 0$ gives the "trivial" solutions $(x, y, \ell) = (0, d(d+1)/2, 2)$, and no solutions for odd ℓ. Likewise the value $x = -1$ for $d \geq 3$ yields the trivial solutions $(x, y, \ell) = (-1, (d-1)d/2, 2)$ and no solutions for odd ℓ. In the case $d = 2$, we have a solution for all $\ell \geq 2$, namely $(-1, 1, \ell)$. This case will be treated separately in Chapter 4.

(ii) For odd exponents ℓ, there is a symmetry between the solutions to (2.6):

$$(x, y, \ell) \longleftrightarrow (-x - d - 1, -y, \ell).$$

This allows us to deduce, from Table 2.1 and (i), all solutions with $x \leq -d-1$.

(iii) The solutions with $-d \leq x \leq -2$ lead to non-negative solutions with smaller values of d through cancellation (and possibly applying the symmetry in (ii)).

Of course arbitrary perfect powers that are sums of at most 50 consecutive cubes can be deduced from our list of ℓ-th powers with ℓ prime.

2.3 Some Very Important Identities

A sum of d consecutive cubes can be written as

$$(x+1)^3 + (x+2)^3 + \cdots + (x+d)^3 = \left(dx + \frac{d(d+1)}{2}\right)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right).$$

Thus, to prove Theorem 2.1.1, we need to solve the Diophantine equation

$$\left(dx + \frac{d(d+1)}{2}\right)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) = y^\ell, \tag{2.7}$$

with ℓ prime and $2 \leq d \leq 50$. We find it convenient to rewrite (2.7) as

$$d(2x + d + 1)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) = 2y^\ell. \tag{2.8}$$

We will use a descent argument together with the identity

$$4\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) - (2x + d + 1)^2 = d^2 - 1. \tag{2.9}$$

to reduce (2.8) to a family of ternary equations. We will explicitly solve these equations through a combination of techniques which include, but are not limited to, descent, lower bounds for linear forms in logarithms and modularity of Galois representations.

Tea and honey is a very grand thing.

Winnie the Pooh, A. A. Milne

Chapter 3

The Case $\ell = 2$: An Elliptic Curve

In this section, we treat the case $\ell = 2$ separately. In this case, we are able to reduce the problem to computing integer points on Elliptic curves. Although this case has been resolved by Stroeker [1995], we provide details and some background on elliptic curves. The computational aspect is in itself interesting, and we will provide a short discussion on this topic. A secondary motivation for elongating this chapter is in order to set up the relevant notation which will be handy when it comes to discussing the modular method.

3.1 Background: Elliptic Curves

This section primarily follows [Silverman, 2009, Chapter III]. We adopt some of their notation for consistency. In this thesis, we will usually work with elliptic curves defined over the rational field, unless otherwise stated. Hence, the results in this section are stated for elliptic curves over the rational field. The results can be extended to elliptic curves over number fields and remain true with the appropriate modifications.

For us an elliptic curve $E/\mathbb{Q}$ is a smooth projective curve in $\mathbb{P}^2$ which in affine coordinates is given by a *long Weierstrass equation*,

$$E \ : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{3.1}$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. Remember that in projective coordinates, we still have the marked point at infinity, given projectively by $\mathcal{O} = [0 : 1 : 0]$.

Completing the square for the variable Y and making the substitution $Y \to$

$\frac{1}{2}(Y - a_1X - a_3)$ gives us the following *medium Weierstrass equation*,

$$E \ : \ Y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3 \qquad \text{and} \qquad b_6 = a_3^2 + 4a_6.$$

The Discriminant and j-invariant of an elliptic curve in medium Weierstrass form are given by

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \qquad \text{and} \qquad j := c_4^3/\Delta,$$

where

$$b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \qquad \text{and} \qquad c_4 = b_2^2 - 24b_4.$$

The smoothness of the Weierstrass model (which forms part of the definition of the elliptic curve) is equivalent to $\Delta \neq 0$. The set of rational points on E is denoted by $E(\mathbb{Q})$. This consists of the point at infinity, together with affine points $(x, y) \in \mathbb{Q}^2$ satisfying the Weierstrass equation. There is a group operation on E (see [Silverman, 2009, Chapter III] for definition). This makes $E(\mathbb{Q})$ into an abelian group with $\mathcal{O}$ as identity; this is called the Mordell–Weil group.

Theorem 3.1.1 (Mordell–Weil)**.** *The group $E(\mathbb{Q})$ is finitely generated. Thus we may write*

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{tors}$ is the torsion subgroup (points of finite order, which are finite) and r is the rank of $E/\mathbb{Q}$ (a non-negative integer).

For a proof of Theorem 3.1.1 see [Silverman, 2009, Chapter VIII].

3.1.1 Integer Points on Elliptic Curves

This subsection primarily follows [Silverman, 2009, Chapter IX] and we continue to adopt their notation for consistency.

The Mordell-Weil theorem shows that an elliptic curve could have infinitely many rational points when the rank is non-zero. However, can we say something about the related topic of *integral points* on elliptic curves? In this subsection, E is an elliptic curve given by a long Weierstrass model as in (3.1) with $a_i \in \mathbb{Z}$ and we address the following questions:

1. How many integer points does E have?

2. Are there finitely many of them?

3. Can we list all of them? (i.e. perform a finite computation)

We begin this subsection with a result of Siegel that addresses question 2 and answers it positively. Siegel provided two proofs to Theorem 3.1.2 by means of *Diophantine approximation*. Both proofs are *ineffective* due to the method used. Siegel answered yes to question 2, but neither proof gives an explicit computable upper bound for the size of such a point, called the *height*. Therefore, questions 1 and 3 still remain unanswered for the moment.

Theorem 3.1.2 (Siegel)**.** *There are finitely many integral points on $E/\mathbb{Q}$.*

Siegel's second proof reduced the problem of finding integer points on elliptic curves to looking for solutions of some S-unit equations. Using Baker's theory of linear forms in logarithms in addition to Siegel's proof provides positive answers to questions 1 and 3, with the answer to 3 being yes in theory. Baker's theory usually churns out extremely large upper bounds for the height. We will shortly see an example of this, thus leaving us with a sense of *"did we really answer question 3 in the positive?"*

Theorem 3.1.3 (Baker)**.** *Let K be a number field. Let $\alpha_1, \ldots, \alpha_n \in K^*$ and $\beta_1, \ldots, \beta_n \in K$. For any constant ν, define*

$$\begin{aligned}\tau(\nu) :&= \tau(\nu; \alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n) \\ &= h([1, \beta_1, \ldots, \beta_n])h([1, \alpha_1, \ldots, \alpha_n])^\nu.\end{aligned}$$

where h is a logarithmic height function. Fix an embedding $K \subset \mathbb{C}$ and let $|\cdot|$ be the corresponding absolute value. Assume that

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0.$$

Then there are effectively computable constants $C, \nu > 0$ which depend only on n and $[K : \mathbb{Q}]$ such that

$$|\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| > C^{-\tau(\nu)}.$$

Proof. See Baker [1990], Section 5.2, page 257. □

3.1.2 Baker Bounds for our Consecutive Cubes

Baker's theory gives effective, yet rather large, bounds for Siegel's theorem. We shall demonstrate by studying what happens to our consecutive cubes. For the following theorem see [Baker, 1990, page 45] or [Silverman, 2009, page 261].

Theorem 3.1.4 (Baker)**.** *Let $A, B, C, D \in \mathbb{Z}$ satisfy $\max\{|A|, |B|, |C|, |D|\} \leq H$. Assume that*

$$E := Y^2 = AX^3 + BX^2 + CX + D$$

is an elliptic curve. Then any integer point $P = (x, y) \in \mathbb{Z}^2$ on E satisfies

$$\max\{|x|, |y|\} < \exp\left(\left(10^6 H\right)^{10^6}\right) := BB.$$

Let $\ell = 2$ in equation (2.7). We can expand the left hand side to get;

$$E_d \ : \ y^2 = dx^3 + \frac{3}{2}d(d+1)x^2 + \frac{d}{2}(d+1)(2d+1)x + \frac{d^2}{4}(d+1)^2.$$

We can apply Theorem 3.1.4 to see what astronomical bounds we can naively expect in computations. For our range, $2 \leq d \leq 50$, we compute the minimum and maximum values for BB that we obtain. In this calculation we see that the smallest Baker bound obtained is still pretty huge!

d	H	Baker Bound
2	15	$1.8157\cdots \times 10^{7,176,091}$
50	$1,625,625$	$2.3417\cdots \times 10^{12,211,020}$

Table 3.1: Baker Bounds

Fortunately for us, substantial help and improvement comes from *linear forms in elliptic logarithms* to significantly reduce the Baker bound; see Smart [1998] for details. The method of linear forms in elliptic logarithms is implemented in `Magma` and can compute integral points on Weierstrass models, provided a Mordell–Weil basis can be determined (which is often the case in practice). One expresses an integral point P on E as a linear combination of a fixed Mordell–Weil basis where Baker's bounds for P translate into bounds for the coefficients of this linear combination. The method then repeatedly uses the LLL algorithm to dramatically reduce the bounds for these coefficients until we are simply able to enumerate the possibilities for P and check integrality.

3.2 Application: Finding Solutions!

Although Theorem 2.1.1 with $\ell = 2$ follows from Stroeker [1995], we explain briefly how this can now be done with the help of an appropriate computer algebra package.

Let (x, y) be an integral solution to (2.7) with $\ell = 2$. Write $X = dx$, and $Y = dy$. Then (X, Y) is an integral point on the elliptic curve

$$E_d \; : \; Y^2 = \left(X + \frac{d^2 + d}{2}\right)\left(X^2 + (d^2 + d)X + \frac{d^4 + d^3}{2}\right).$$

Using the computer algebra package `Magma` [Bosma et al. [1997]], we determined the integral points on E_d for $2 \leq d \leq 50$. For this computation, `Magma` applies the standard linear forms in elliptic logarithms method [Smart, 1998, Chapter XIII], which is the same method used by Stroeker (though the implementation is independent). From this we immediately recover the original solutions (x, y) to (2.7) with $\ell = 2$, and the latter are found in our Table 2.1. We have checked that our solutions with $\ell = 2$ are precisely those given by Stroeker.

We shall henceforth restrict ourselves to $\ell \geq 3$ for the remainder of Part I of this thesis.

Chapter 4

The Case $d = 2$: Applying the Results of Nagell

Our method for general d explained in later sections fails for $d = 2$. This is because of the presence of solutions $(x, y) = (-2, -1)$ and $(x, y) = (-1, 1)$ to (2.6) for all $\ell \geq 3$. In this section we treat the case $d = 2$ separately, reducing to Diophantine equations that have already been solved by Nagell.

4.1 Background: The Equations $X^2 + X + 1 = Y^n$ and $X^2 + X + 1 = 3Y^n$

This section is predominantly concerned with the following theorem of Nagell which can be found in Nagell [1921]. A treatment of (4.2) can also be found in [Cohen, 2007a, pages 420–421].

Theorem 4.1.1 (Nagell, 1921)**.** *The only integer solutions to the equation*

$$X^2 + X + 1 = Y^n \tag{4.1}$$

with $n \neq 3^k$ are the trivial ones with $X = -1$ or 0. The only integer solutions to the equation

$$X^2 + X + 1 = 3Y^n \tag{4.2}$$

for $n > 2$ are again the trivial ones with $X = -2, 1$.

4.2 Application: Finding Solutions!

Recall equation (2.6) with $d = 2$ and $\ell \geq 3$ a prime:

$$(x+1)^3 + (x+2)^3 = y^\ell.$$

For convenience, let $z = x+1$. Then, the equation becomes $z^3 + (z+1)^3 = y^\ell$ which can be rewritten as

$$(2z+1)(z^2+z+1) = y^\ell. \tag{4.3}$$

Here y and z are integers and $\ell \geq 3$ is prime. Suppose first that $\ell = 3$. This equation here defines a genus 1 curve. We checked using `Magma` that it is isomorphic to the elliptic curve $Y^2 - 9Y = X^3 - 27$ with Cremona label `27A1`, and that it has Mordell–Weil group (over $\mathbb{Q}$) $\cong \mathbb{Z}/3\mathbb{Z}$. It follows that the only rational points on (4.3) with $\ell = 3$ are the three obvious ones : $(z, y) = (-1/2, 0)$, $(0, 1)$ and $(-1, -1)$. These yield the solutions $(x, y) = (-1, 1)$ and $(x, y) = (-2, -1)$ to (2.6).

We may thus suppose that $\ell \geq 5$ is prime. The resultant of the two factors on the left-hand side of (4.3) is 3 and, moreover, $9 \nmid (z^2+z+1)$.[1] It follows that either

$$2z+1 = y_1^\ell, \qquad z^2+z+1 = y_2^\ell, \qquad y = y_1 y_2 \tag{4.4}$$

or

$$2z+1 = 3^{\ell-1} y_1^\ell, \qquad z^2+z+1 = 3y_2^\ell, \qquad y = 3y_1 y_2. \tag{4.5}$$

By Theorem 4.1.1 the only solutions to equation (4.4) are the trivial ones, $(z, y) = (-1, -1)$ and $(0, 1)$ for any odd prime ℓ. Working back, we recover the solutions $(x, y) = (-2, -1)$ and $(-1, 1)$ for any odd prime ℓ to (2.6).

Again by Theorem 4.1.1, the only solutions to equation (4.5) are the trivial ones, $(z, y_2) = (-2, 1)$ and $(1, 1)$. We have $(z, y) = (-2, -3)$ and $(1, 3)$. Working back, we do not recover a solution for the case $(z, y) = (-2, -3)$. We get $x = -3$ which gives us the following non-perfect power, $(-2)^3 + (-1)^3 = -9$. In the case $(z, y) = (1, 3)$ we yield a solution $(x, y) = (0, 3)$ i.e. $1^3 + 2^3 = 3^2$. However, we are only interested in solutions where $x \geq 1$ for our tables, as explained in Chapter 2. Moreover, for this section, we are under the assumption that $\ell \geq 3$. (The case $\ell = 2$ has already been considered in Chapter 3).

Remark: In Bennett et al. [2017] we incorrectly state that equation $X^2 + X + 1 = 3Y^n$ for $n > 2$ only has the trivial solution with $X = 1$. There is also the

[1] We can check that the congruence $a^2 + a + 1 \equiv 0 \pmod 9$ has no solutions, simply by trying the values $a = 0, \ldots, 8$.

trivial solution $X = -2$. As seen above, considering this solution with our sums of consecutive cubes does not yield a new solution (or any solution in fact with $x \geq 1$), and therefore does not affect Theorem 1 in Bennett et al. [2017].

One of the advantages of being disorganized is that one is always having surprising discoveries.

Winnie the Pooh, A. A. Milne

Chapter 5

First Descent for $\ell \geq 3$

In this chapter, we perform a descent (basically a clever factorisation) for equation (2.8) when $3 \leq d \leq 50$ and $\ell \geq 3$. For each value of d, we are able to perform the descent *uniformly* for all $\ell \geq 5$. By a *uniform descent*, we mean that all factorisations produced are independent of $\ell \geq 5$. This step is essential in producing ternary equations in the correct format to then be amenable to techniques described in later chapters (for example, linear forms in logarithms, Sophie-Germain type methods and the modular approach).

Writing up the descent for individual values of $3 \leq d \leq 50$ would soon become repetitive, with an extremely cluttered exposition. So instead, we get the computer to perform the descent for us. In order to get the computer to do all of the work, we first need to specify *the algorithm*, which is a finite number of calculations that the computer must carry out to show us all of the possible factorisations.[1]

Here is a reminder of equation (2.8):

$$d\,(2x+d+1)\left(x^2+(d+1)x+\frac{d(d+1)}{2}\right)=2y^\ell.$$

Before we state the algorithm, we first give a concrete example to show the types of calculations that can occur.

5.1 An Example: Descent for $d = 5$, $\ell \geq 3$:

Let $d = 5$ and $\ell \geq 5$. Then equation (2.8) in this specific case is

$$5\,(x+3)\left(x^2+6x+15\right)=y^\ell.$$

[1]There are only a finite number of possible factorisations and this will be shown in the forthcoming lemma - in case that was a concern at this stage.

This can be rewritten as

$$(x+3)\left(x^2+6x+15\right) = 5^{\ell-1}w^\ell,$$

where $y = 5w$. First we make a sensible change of variables. This is not necessary and indeed omitted in our algorithm, but for this specific case, it will show the key steps in our algorithm more transparently. We let $z = x + 3$ to get:

$$z\left(z^2+6\right) = 5^{\ell-1}w^\ell.$$

There is an obvious factorisation to the left hand side of the equation. Therefore, we would like to know the factorisation for the right hand side. This is the main idea behind *descent*.

We will need the *resultant* of z and z^2+6, which is equal to 6 in this case, to determine the possible factorisations that can happen on the right hand side. The resultant tells us that the factors on the left hand side, z and z^2+6 have a greatest common divisor (abbreviated to gcd) that is $1, 2, 3$ or 6. We are using a key fact here: the gcd between two polynomials divides the resultant.

Notice that we have $5^{\ell-1}$ on the right hand side. Translating this information to the left hand side, we see that either $5^{\ell-1}$ divides z or it divides z^2+6: 5 cannot divide both z and z^2+6, otherwise we contradict the information about their gcd obtained from calculating the resultant.

We are ready to state all of the possible equations obtained from the first[2] descent. We can conveniently split the cases into two: When $5 \mid z$ and when $5 \nmid z$. We let $\alpha = \gcd(z, 6)$. Thus, $\alpha \in \{1, 2, 3, 6\}$.

Case $5 \mid z$: In this case

$$z = 5^{\ell-1}\alpha^{\ell-1}y_1^\ell, \qquad z^2+6 = \alpha y_2^\ell,$$

where y_1 and y_2 are integers and $w = \alpha y_1 y_2$.

Case $5 \nmid z$: In this case

$$z = \alpha^{\ell-1}y_1^\ell, \qquad z^2+6 = 5^{\ell-1}\alpha y_2^\ell,$$

where again y_1 and y_2 are integers and $w = \alpha y_1 y_2$.

Remark: In performing the descent when $d = 5$, one may notice that this is completely independent of ℓ when $\ell \geq 5$. After the descent, we have a total of 8

[2]Yes, you have guessed it! There is a second descent coming soon!

cases, or equations, to consider. In performing the descent for all $3 \leq d \leq 50$ and $\ell \geq 5$, we split our equation up into different cases and hence obtain 906 ternary equations to solve in the variables (y_1, y_2, ℓ).[3] The argument in the next section is only for $\ell \geq 5$ and will need modification for $\ell = 3$, which we carry out in Section 5.3.

5.2 The Algorithm: A Uniform Descent for $\ell \geq 5$

Let $d \geq 3$. We consider equation (2.8) with exponent $\ell \geq 5$. In this section, we determine the algorithm to perform a uniform descent for any value of $d \geq 3$ which is independent of $\ell \geq 5$. As stated previously, the argument in this section will need modification for $\ell = 3$ which we carry out in Section 5.3.

For a prime q we let

$$\mu_q = \mathrm{ord}_q(d^2 - 1) \quad \text{and} \quad \nu_q = \mathrm{ord}_q(d), \tag{5.1}$$

i.e. the exponent of the largest power of q dividing $d^2 - 1$ and d, respectively. We associate to q a finite subset $T_q \subset \mathbb{Z}^2$ as follows.

- If $q \nmid d(d^2 - 1)$ then let $T_q = \{(0, 0)\}$.
- For $q = 2$ we define

$$T_2 = \begin{cases} \{(0, 1 - \nu_2)\} & \text{if } 2 \mid d \\ \{(1, 0),\ (\mu_2/2, 1 - \mu_2/2),\ (3 - \mu_2, \mu_2 - 2)\} & \text{if } 2 \nmid d \text{ and } 2 \mid \mu_2 \\ \{(1, 0),\ (3 - \mu_2, \mu_2 - 2)\} & \text{if } 2 \nmid d \text{ and } 2 \nmid \mu_2. \end{cases}$$

- For odd $q \mid d$, let

$$T_q = \{(-\nu_q, 0),\ (0, -\nu_q)\}.$$

- For odd $q \mid (d^2 - 1)$, let

$$T_q = \begin{cases} \{(0, 0),\ (-\mu_q, \mu_q),\ (\mu_q/2, -\mu_q/2)\} & \text{if } 2 \mid \mu_q, \\ \{(0, 0),\ (-\mu_q, \mu_q)\} & \text{if } 2 \nmid \mu_q. \end{cases}$$

We take $\mathcal{A}_d$ to be the set of pairs of positive rationals (α, β) such that

$$(\mathrm{ord}_q(\alpha), \mathrm{ord}_q(\beta)) \in T_q$$

[3] Solving for $(y_1, y_2, \ell) \in \mathbb{Z}^3$ will eventually give us an $(x, y, \ell) \in \mathbb{Z}^3$ solution to equation (2.8).

for all primes q. It is clear that $\mathcal{A}_d$ is a finite set, which is, in practice, easy to write down for any value of d.

Lemma 5.2.1. *Let (x, y) be a solution to (2.8) where $\ell \geq 5$ is a prime. Then there are rationals y_1, y_2 and a pair $(\alpha, \beta) \in \mathcal{A}_d$ such that*

$$2x + d + 1 = \alpha y_1^\ell, \qquad x^2 + (d+1)x + \frac{d(d+1)}{2} = \beta y_2^\ell. \tag{5.2}$$

Moreover, if $3 \leq d \leq 50$ then y_1 and y_2 are integers.

Remark: The reader will observe that the definition of $\mathcal{A}_d$ is independent of ℓ. Thus, given d, the lemma provides us with a way of carrying out the descent uniformly for all $\ell \geq 5$.

Proof. Let us first assume the first part of the lemma and deduce the second. Using a short `Magma` script, we wrote down all possible pairs $(\alpha, \beta) \in \mathcal{A}_d$ for $3 \leq d \leq 50$ and checked that

$$\max\{\mathrm{ord}_q(\alpha),\ \mathrm{ord}_q(\beta)\} \leq 4$$

for all primes q. As x is an integer, we know from (5.2) that

$$\mathrm{ord}_q(\alpha) + \ell\,\mathrm{ord}_q(y_1) \geq 0 \quad \text{and} \quad \mathrm{ord}_q(\beta) + \ell\,\mathrm{ord}_q(y_2) \geq 0,$$

for all primes q. Since $\ell \geq 5$, it is clear that $\mathrm{ord}_q(y_1) \geq 0$ and $\mathrm{ord}_q(y_2) \geq 0$ for all primes q. This proves the second part of the lemma.

We now prove the first part of the lemma. For $2x + d + 1 = 0$ (which can only arise for odd values of d) we can take $y_1 = 0$, $y_2 = 1$,

$$\alpha = \frac{8}{d(d^2-1)} \quad \text{and} \quad \beta = \frac{d^2-1}{4}; \tag{5.3}$$

it is easy to check that this particular pair (α, β) belongs to $\mathcal{A}_d$. We shall henceforth suppose that $2x + d + 1 \neq 0$.

Claim: Let q be a prime and define

$$\epsilon = \mathrm{ord}_q(2x + d + 1) \quad \text{and} \quad \delta = \mathrm{ord}_q\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right).$$

Then $(\epsilon, \delta) \equiv (\epsilon', \delta') \mod \ell$ for some $(\epsilon', \delta') \in T_q$.

To complete the proof of Lemma 5.2.1, it is clearly enough to prove this claim. From (2.8) and (2.9), the claim is certainly true if $q \nmid d(d^2-1)$, so we may

suppose that $q \mid d(d^2-1)$. Observe that for any q, from (2.8),

$$\nu_q + \epsilon + \delta \equiv \mathrm{ord}_q(2) \mod \ell\,. \tag{5.4}$$

Moreover, from (2.9),

$$\mu_q \geq \min(2\epsilon,\ \delta + 2\,\mathrm{ord}_q(2)) \qquad \text{with equality if } \ 2\epsilon \neq \delta + 2\,\mathrm{ord}_q(2). \tag{5.5}$$

We deal first with the case where $q = 2 \mid d$ (so that $\epsilon = 0$). By (5.4), we obtain that $(\epsilon, \delta) \equiv (0, 1-\nu_2) \mod \ell$, and, by definition, $T_2 = \{(0, 1-\nu_2)\}$ establishing our claim. Next we suppose that $q = 2 \nmid d$ (in which case $\nu_2 = 0$):

- If $2\epsilon = \delta + 2$ then, from (5.4) and the fact that $\ell \geq 5$, we obtain $(\epsilon, \delta) \equiv (1, 0) \mod \ell$.
- If $2\epsilon > \delta + 2$ then, from (5.5), we have $\mu_2 = \delta + 2$, so from (5.4) we obtain $(\epsilon, \delta) \equiv (3 - \mu_2, \mu_2 - 2) \mod \ell$.
- If $2\epsilon < \delta + 2$ then, from (5.5), we have $\mu_2 = 2\epsilon$, so from (5.4) we obtain $(\epsilon, \delta) \equiv (\mu_2/2, 1 - \mu_2/2) \mod \ell$.

Next, let us next consider odd $q \mid d$ (whereby we have that $\mu_q = 0$). From (5.5), it follows that either $\epsilon = 0$ or $\delta = 0$. From (5.4), we obtain $(\epsilon, \delta) \equiv (0, -\nu_q)$ or $(-\nu_q, 0) \mod \ell$ as required.

Finally we consider odd $q \mid (d^2-1)$ (so $\nu_q = 0$):

- If $2\epsilon = \delta$ then, from (5.4) and the fact that $\ell \geq 5$, we obtain $(\epsilon, \delta) \equiv (0, 0) \mod \ell$.
- If $2\epsilon > \delta$ then, from (5.5), we have $\mu_q = \delta$, so from (5.4) we obtain $(\epsilon, \delta) \equiv (-\mu_q, \mu_q) \mod \ell$.
- If $2\epsilon < \delta$ then, from (5.5), we have $\mu_q = 2\epsilon$, so from (5.4) we obtain $(\epsilon, \delta) \equiv (\mu_q/2, -\mu_q/2) \mod \ell$.

□

From (5.2) and (2.9), we deduce the following ternary equation

$$4\beta y_2^{\ell} - \alpha^2 y_1^{2\ell} = d^2 - 1. \tag{5.6}$$

We need to solve this for each possible $(\alpha, \beta) \in \mathcal{A}_d$ with $2 \leq d \leq 50$ and y_1, y_2 integers. Clearing denominators and dividing by the greatest common divisor of the

coefficients we can rewrite this as

$$ry_2^{\ell} - sy_1^{2\ell} = t \tag{5.7}$$

where r, s, t are positive integers and $\gcd(r, s, t) = 1$.

5.3 The Algorithm: Descent for $\ell = 3$

In this section we modify the approach of Section 5.2 to deal with equation (2.8) with exponent $\ell = 3$.

For an integer m, we denote by $[m]$ the element in $\{0, 1, 2\}$ such that $m \equiv [m] \bmod 3$. For a prime q we let μ_q and ν_q be as in (5.1). For each prime q, we define a finite subset $T_q \subset \{(m, n) : m, n \in \{0, 1, 2\}\}$.

- If $q \nmid d(d^2 - 1)$ then let $T_q = \{(0, 0)\}$.
- For $q = 2$ we let

$$T_2 = \begin{cases} \{(0,\, [1 - \nu_2])\} & \text{if } 2 \mid d \\ \{(1,0),\ (0,1),\ (2,2)\} & \text{if } 2 \nmid d \text{ and } \mu_2 \geq 4. \\ \{(1,0),\ (0,1)\} & \text{if } 2 \nmid d \text{ and } \mu_2 = 3. \end{cases}$$

- For odd $q \mid d$, let

$$T_q = \{([-\nu_q],\, 0),\ (0,\, [-\nu_q])\}.$$

- For odd $q \mid (d^2 - 1)$, let

$$T_q = \begin{cases} \{(0,0),\ (1,2),\ (2,1)\} & \text{if } \mu_q \geq 2 \\ \{(0,0),\ (2,1)\} & \text{if } \mu_q = 1. \end{cases}$$

Let $\mathcal{A}_d$ be the set of pairs of positive integers (α, β) such that $(\mathrm{ord}_q(\alpha), \mathrm{ord}_q(\beta)) \in T_q$ for all primes q.

Lemma 5.3.1. *Let (x, y) be a solution to (2.8) where $\ell = 3$ a prime. Then there are integers y_1, y_2 and a pair $(\alpha, \beta) \in \mathcal{A}_d$ such that (5.2) holds.*

Proof. The proof is an easy adaptation of the proof of Lemma 5.2.1. We omit the details. □

5.4 Proof of Theorem 2.1.1: Descent for $\ell = 3$

From this lemma and (2.9) we reduce the resolution of (2.8) with $\ell = 3$ to solving a number of equations of the form (5.6). These can be transformed by clearing denominators and dividing by the greatest common divisor of the coefficients into equations of the form (5.7) where r, s, t are positive integers and $\gcd(r, s, t) = 1$. An implementation of above procedure leaves us with 942 quintuples (d, ℓ, r, s, t) with $\ell = 3$.

We emphasise in passing the difference between the approach of subsection 5.2 and 5.3; the former gives the same set of triples (r, s, t) for all exponents $\ell \geq 5$, whereas the latter gives a possibly different set of triples (r, s, t) for $\ell = 3$. The reason for this is if the tuple (r, s, t) contains some cubes or higher powers, then any cubes dividing r can be absorbed into the unknown y_2 or any sixth powers dividing s can be absorbed into the unknown y_2 since we are in the case $\ell = 3$.

"I don't feel very much like Pooh today," said Pooh.
"There, there," said Piglet.
"I'll bring you tea and honey until you do."

Winnie the Pooh, A. A. Milne

Chapter 6

Linear Forms in Logarithms

The descent step in the previous chapter transforms (2.8) into a family of ternary equations (5.6). In this section, we appeal to lower bounds for linear forms in logarithms to find an explicit upper bound for the exponent ℓ appearing in these equations.

We have already seen an example of the application of linear forms in logarithm in Chapter 3, Subsection 3.1.1. This chapter requires us to use the specific case of *linear forms in two logarithms*.

The first section of this chapter, Section 6.1, uses a theorem in Cohen [2007b] to give us a naive bound for ℓ. It turns out that this bound is better than that given in Bennett et al. [2017]. The focus of the remainder of this chapter then turns to the original work by Bennett et al. [2017]. We expand on the details since the calculations are very explicit, and some of the intricate workings of linear forms in two logarithms become extremely transparent.

6.1 A Naive Bound: Linear Forms in Two Logarithms

In this section, we follow [Cohen, 2007b, Chapter 12, p. 423]. We begin by stating a theorem due to Mignotte and then apply the theorem to our ternary equations.

Theorem 6.1.1 (Mignotte)**.** *Assume that the exponential Diophantine inequality*

$$|ax^n - by^n| \leq c, \qquad \text{with } a, b, c \in \mathbb{Z}_{\geq 0} \text{ and } a \neq b,$$

has a solution in strictly positive integers x and y with $\max\{x, y\} > 1$. Let $A = \max\{a, b, 3\}$. Then

$$n \leq \max\left\{3\log\left(1.5|c/b|\right),\ \frac{7400\log A}{\log\left(1 + \log A/\log\left(|\ a/b\ |\right)\right)}\right\}.$$

Remark: If $A = b$ and $a = 1$, then $\log A / \log(|\, a/b \,|) = -1$. Therefore, our denominator becomes $\log(1-1) = \log(0)$. Since the original Diophantine inequality is $|ax^n - by^n| \leq c$, we may swap the terms ax^n and by^n. Appropriate relabelling gives us $A = a$ and $b = 1$ to overcome this problem.

6.1.1 Naive Bounds for our Sums of Consecutive Cubes

From the previous section, recall equation (5.7):

$$ry_2^{\ell} - sy_1^{2\ell} = t$$

where r, s, t are positive integers and $\gcd(r, s, t) = 1$. The descent step of the previous section left us with a finite set of (r, s, t) tuples, which were obtained from the finite pairs $(\alpha, \beta) \in \mathcal{A}_d$ for $3 \leq d \leq 50$. Checking all of the tuples (r, s, t) with Theorem 6.1.1 in `Magma`, we see that the maximum value of ℓ occurs at $d = 50$, where we obtain the bound:

$$\ell \leq 986,053.$$

Remark: This procedure leaves us with only one exceptional tuple when $d = 8$ and $(r, s, t) = (1, 1, 63)$ for which Theorem 6.1.1 cannot be applied (in this instance, the condition $a \neq b$ is violated). Notice that the corresponding values of α and β are $(1, 1/4)$.[1] For $(r, s, t) = (1, 1, 63)$, we want to solve $y_2^{\ell} - y_1^{2\ell} = 63$. Let's change variables and let $x := y_1^{\ell}$. Then we want to find all integer solutions to $x^2 + 63 = y_2^{\ell}$, which has already been solved in the literature (see Bugeaud et al. [2006]). It has solutions

$$(|x|, |y|, \ell) = (1, 4, 3),\ (13537, 568, 3),\ (31, 4, 5),\ (1, 2, 6),\ (31, 2, 10).$$

Noting that 13537 and 31 are prime, and $x = y_1^{\ell}$, means that ℓ must be equal to 1. Hence, we do not yield solutions for our sum of 8 consecutive cubes in these cases. On the other hand, the solutions $(1, 4, 3)$ and $(1, 2, 6)$ yield essentially same solution: namely $63 = 1 + 4^3 = 1 + 2^6$. Undoing the descent step that occurred in the previous chapter, we have $y = \alpha\beta y_1 y_2 = 4^3$. Going right back to the beginning of our calculations, we are able to solve the equation (for a sum of 8 consecutive cubes being a perfect power) in the indeterminate x:

$$(x+1)^3 + \cdots + (x+8)^3 = 4^3,$$

[1] This case also arises as an exceptional case in Section 6.3.

where we find the solution $x = -4$. Noting that our table only shows solutions when $x \geq 1$, we are done.

6.2 A Result of Laurent for Linear Forms in Two Logarithms

In this section, we require a result of Laurent on linear forms in two logarithms of algebraic numbers. By an *algebraic number* we mean an element of $\alpha \in \mathbb{C}$, which is the root of a non-zero polynomial with rational coefficients. If we choose the non-zero polynomial in $\mathbb{Q}[x]$ with minimal degree, then this is irreducible, and is called the *minimal polynomial* of α. The minimal polynomial is unique up to scaling, and is usually taken to be monic. In this subject (linear forms in logarithms) however, the minimal polynomial is scaled so that the coefficients are integers, but their gcd is 1. Let α have minimal polynomial $f(x)$ given by:

$$f(x) := a_d x^d + \cdots + a_0 = 0, \qquad a_i \in \mathbb{Z}$$

where $\gcd(a_0, \ldots, a_d) = 1$ and $a_d \neq 0$. Let $\alpha^{(i)}, \ldots, \alpha^{(d)}$ be the roots of $f(x)$ in $\mathbb{C}$; these are the *conjugates* of α. We define the *absolute logarithmic height* of an algebraic number α by:

$$h(\alpha) = \frac{1}{d}\left(\log|a_d| + \sum_{i=1}^{d} \log\max(1, |\alpha^i|)\right).$$

Definition 6.2.1. *For non-zero algebraic numbers α and β, we say that they are multiplicatively independent if the only solution to $\alpha^m\beta^n = 1$ with m, $n \in \mathbb{Z}$ is $(m, n) = (0, 0)$.*

Lemma 6.2.2. *If α and β are positive real algebraic numbers that are multiplicatively dependent, then there are coprime integers u and v, which are not both zero, such that $\alpha^u = \beta^v$.*

Proof. As α and β are algebraically dependent, there are integers m and n, not both zero such that $\alpha^m\beta^n = 1$. Let $g = \gcd(m, n)$. Let $u = m/g$ and $v = -n/g$, so that u and v are coprime integers and not both zero. Then we can rewrite $\alpha^m\beta^n$ as $(\alpha^u/\beta^v)^g = 1$. Thus α^u/β^v is a g-th root of unity. However, α^u/β^v is real and positive, so $\alpha^u/\beta^v = 1$, which gives the lemma. □

We will use a special case of Corollary 2 in Laurent [2008] (with $m = 10$ in the notation of that paper):

Proposition 6.2.3 (Laurent)**.** *Let α_1 and α_2 be positive real algebraic numbers. Write*

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$$

and let A_1 and A_2 be real numbers, both strictly greater than 1 such that

$$\log A_i \geq \max\{h(\alpha_i), |\log \alpha_i|/D, 1/D\}, \qquad i = 1, 2.$$

Let b_1 and b_2 be positive integers and write $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$ (our linear form in two logarithms). Let

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}\,.$$

Then

$$\log|\Lambda| \geq -25.2D^4 \left(\max\{\log b' + 0.38, 10/D, 1\}\right)^2 \log A_1 \log A_2.$$

6.3 Application of Linear Forms in Two Logarithms

In this section, we will assume that $3 \leq d \leq 50$. Keeping with the notation of Chapter 5, (α, β) will denote an element of $\mathcal{A}_d$ while (y_1, y_2) denotes an integral solution to (5.6). By definition of $\mathcal{A}_d$, the rationals α and β are both positive. It follows from (5.6) that $y_2 > 0$. We will apply Proposition 6.2.3 to deduce a bound on the exponent ℓ in (5.6).

Lemma 6.3.1. *Let $\ell > 1000$. Suppose $|y_1|$, $y_2 \geq 2$ and $y_2 \neq y_1^2$. Let*

$$\alpha_1 = 4\beta/\alpha^2 \quad \textit{and} \quad \alpha_2 = y_1^2/y_2. \tag{6.1}$$

Then α_1 and α_2 are positive and multiplicatively independent. Moreover, writing

$$\Lambda = \log \alpha_1 - \ell \log \alpha_2, \tag{6.2}$$

we have

$$0 < \Lambda < \frac{d^2 - 1}{\alpha^2 y_1^{2\ell}}. \tag{6.3}$$

Proof. By the observation preceding the statement of the lemma, we know that α_1 and α_2 are positive. From (5.6), (6.1), (6.2) and (6.3), we have

$$e^{\Lambda} - 1 = \frac{4\beta}{\alpha^2} \cdot \frac{y_2^{\ell}}{y_1^{2\ell}} - 1 = \frac{d^2 - 1}{\alpha^2 y_1^{2\ell}} > 0.$$

Thus $\Lambda > 0$. The second part of the lemma thus follows from the inequality $e^{\Lambda} - 1 >$

Λ which we get from the power series expansion $e^\Lambda = 1 + \Lambda + \Lambda^2/2! + \cdots$.

It remains to show the multiplicative independence of α_1 and α_2 so suppose, for a contradiction, that they are are multiplicatively dependent. By Lemma 6.2.2 there exist coprime integers u and v, not both zero, such that $\alpha_1^u = \alpha_2^v$.

If $\alpha_1 = 1$ then $\alpha^2 = 4\beta$ by (6.1). By (5.6) we have[2]

$$y_2^\ell - y_1^{2\ell} = \frac{d^2-1}{\alpha^2}.$$

As $3 \le d \le 50$, we see that $y_2 \ge y_1^2 + 1$ and

$$2499 \ge \frac{d^2-1}{\alpha^2} \ge (y_1^2+1)^\ell - y_1^{2\ell} \ge \ell y_1^2 \ge 4000$$

as $\ell > 1000$ and $|y_1| \ge 2$. This gives a contradiction.

Therefore $\alpha_1 \ne 1$. If p is a prime then

$$u \cdot \mathrm{ord}_p(\alpha_1) = v \cdot \mathrm{ord}_p(\alpha_2).$$

As u and v are coprime, we see that $v \mid \mathrm{ord}_p(\alpha_1)$. Define

$$g = \gcd\{\mathrm{ord}_p(\alpha_1) \,:\, p \text{ prime dividing the numerator or denominator of } \alpha\}.$$

As $\alpha_1 \ne 1$, there will certainly be primes dividing either the numerator or the denominator of α and so $g \ne 0$. Clearly $v \mid g$. However, from (6.2),

$$|\Lambda| = |\log \alpha_1| \cdot \left|1 - \ell \frac{\log \alpha_2}{\log \alpha_1}\right| = |\log \alpha_1| \cdot \left|1 - \ell \frac{u}{v}\right|.$$

From (6.3), we have

$$0 < \left|1 - \ell \frac{u}{v}\right| < \frac{d^2-1}{|\log \alpha_1| \cdot \alpha^2 y_1^{2\ell}}.$$

Now the non-zero rational $1 - \ell u/v$ has denominator dividing v and hence dividing g. Thus,

$$\frac{1}{g} \le \left|1 - \ell \frac{u}{v}\right|.$$

Since $|y_1| \ge 2$, it follows that

$$4^\ell \le y_1^{2\ell} < \frac{(d^2-1)g}{|\log \alpha_1| \cdot \alpha^2},$$

[2] In subsection 6.1.1 the case $r = s = 1$ which is equivalent to $\alpha^2 = 4\beta$ also arose as an exceptional case, which only occurred in the case $d = 8$. This case was resolved separately in subsection 6.1.1 by reducing to equations already solved in the literature by Bugeaud et al. [2006].

and so

$$\ell < \log\left(\frac{(d^2-1)g}{|\log\alpha_1|\cdot\alpha^2}\right)/\log 4\,.$$

We wrote a simple `Magma` script that computes this bound on ℓ for the values of d in the range $3 \le d \le 50$ and the possible pairs $(\alpha,\beta) \in \mathcal{A}_d$ with corresponding $\alpha_1 = 4\beta/\alpha^2 \ne 1$. We found that the largest possible value for the right-hand side of the inequality is $19.09\ldots$ corresponding to $d = 50$ and $(\alpha,\beta) = (1/62475, 2499)$. As $\ell > 1000$, we have a contradiction by a wide margin.

In fact, we found only one pair (α,β) for which $\alpha_1 = 1$. This arises when $d = 8$ and $(\alpha,\beta) = (1, 1/4)$. □

Lemma 6.3.2. *Let $A_2 = \max\{y_1^2,\, y_2\}$. Under the notation and assumptions of the previous lemma,*

$$1 \;\le\; \frac{\log A_2}{\log y_1^2} \;\le\; 1.03.$$

Proof. It is sufficient to show that $\log y_2/\log y_1^2 \le 1.03$. From (6.1), (6.2) and (6.3), we have

$$\log\alpha_1 - \ell(\log y_1^2 - \log y_2) \;<\; \frac{d^2-1}{\alpha^2\cdot 4^\ell}$$

where we have used the assumption $|y_1| \ge 2$. It follows that

$$\begin{aligned}\frac{\log y_2}{\log y_1^2} &< 1 + \frac{1}{\ell\log y_1^2}\left(-\log\alpha_1 + \frac{(d^2-1)}{\alpha^2\cdot 4^\ell}\right)\\ &\le 1 + \frac{1}{\ell\log y_1^2}\left(|\log\alpha_1| + \frac{(d^2-1)}{\alpha^2\cdot 4^\ell}\right)\\ &< 1 + \frac{1}{1000\log 4}\left(|\log\alpha_1| + \frac{(d^2-1)}{\alpha^2\cdot 4^{1000}}\right),\end{aligned}$$

using the assumptions $\ell > 1000$ and $|y_1| \ge 2$. We wrote a `Magma` script that computed this upper bound for $\log y_1^2/\log y_2$ for all $3 \le d \le 50$ and $(\alpha,\beta) \in \mathcal{A}_d$. The largest value of the upper bound we obtained was $1.02257\ldots$, again corresponding to $d = 50$ and $(\alpha,\beta) = (1/62475, 2499)$. This completes the proof. □

We continue under the assumptions of Lemma 6.3.1, applying Proposition 6.2.3 to obtain a bound for the exponent ℓ. We let

$$A_1 = \max\{H(\alpha_1),\, e\},$$

where $H(u/v)$, for coprime integers u, v (with v non-zero) is simply $\max\{|u|, |v|\}$. Let A_2 be as in Lemma 6.3.2. We see, thanks to Lemma 6.3.1, that the hypotheses

of Proposition 6.2.3 are satisfied for our choices of α_1, α_2, A_1, A_2 with $D = 1$. We write

$$b' = \frac{1}{\log A_2} + \frac{\ell}{\log A_1} > \frac{1000}{\log A_1}$$

as $\ell > 1000$. We checked that the smallest possible value for $1000/\log A_1$ for $3 \leq d \leq 50$ and $(\alpha, \beta) \in \mathcal{A}_d$ is $31.95\cdots$ arising from the choice $d = 50$ and $(\alpha, \beta) = (1/62475, 2499)$. From Proposition 6.2.3,

$$-\log|\Lambda| < 25.2 \log A_1 \cdot \log A_2 \cdot (\log b')^2 \leq 25.2 \log A_1 \cdot \log A_2 \cdot \log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right),$$

where we have used the fact that $A_2 \geq y_1^2 \geq 4$. Combining this with (6.3), we have

$$\ell \log y_1^2 \ < \ \log\left(\frac{d^2-1}{\alpha^2}\right) + 25.2 \log A_1 \cdot \log A_2 \cdot \log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right).$$

Next we divide by $\log y_1^2$, making use of the fact that $\log A_2/\log y_1^2 < 1.03$ and also that $|y_1| \geq 2$, to obtain

$$\ell \ < \ \frac{1}{\log 4}\log\left(\frac{d^2-1}{\alpha^2}\right) + 26 \log A_1 \cdot \log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right).$$

The only remaining variable in this inequality is ℓ. It is a straightforward exercise in calculus to deduce a bound on ℓ for any d, α and β. In fact the largest bound on ℓ we obtain for d in our range is $\ell < 2,648,167$. We summarize the results of this section in the following lemma.

Lemma 6.3.3. *Let $3 \leq d \leq 50$ and $(\alpha, \beta) \in \mathcal{A}_d$. Let (y_1, y_2) be an integral solution to (5.6) with $|y_1|$, $y_2 \geq 2$ and $y_2 \neq y_1^2$. Then $\ell < 3 \times 10^6$.*

6.3.1 Proof of Theorem 2.1.1: Bounding ℓ

We have dealt with the cases $\ell = 2$ and $d = 2$ in Chapters 3 and 4 respectively, and so $\ell \geq 3$ and $3 \leq d \leq 50$. We dealt with $\ell = 3$ in Section 5.3, so suppose $\ell \geq 5$. Lemma 5.2.1 provides a finite set $\mathcal{A}_d$ of pairs (α, β) such that for every solution (x, y) of equation (2.8), there is a pair $(\alpha, \beta) \in \mathcal{A}_d$ and integers (y_1, y_2) satisfying equations (5.2), (5.6) and (5.7). Lemma 6.3.3 tells us that $\ell < 3 \times 10^6$ provided that the $|y_1|$, $y_2 > 2$ and $y_2 \neq y_1^2$. It is easy to determine (y_1, y_2) for which these conditions fail. Indeed, instead of equation (5.6), consider the equivalent equation (5.7) with integral coefficients. If $y_2 = y_1^2$, then equation (5.7) reduces to $(r - s)y_1^{2\ell} = t$ which allows us to easily determine the corresponding solutions, and similarly for $y_2 = 1$, and for $y_1 \in \{-1, 0, 1\}$. We determined all the solutions

(y_1, y_2) where the hypotheses fail for $3 \leq d \leq 50$ and checked that none of these leads to a solution to equation (2.8) with $x \geq 1$ integral (for the purpose of proving Theorem 2.1.1, we are only interested in $x \geq 1$). Thus we may suppose that the hypotheses of Lemma 6.3.3 hold and conclude that $\ell < 3 \times 10^6$.

"In describing the honourable mission I charged him with, M. Pernety informed me that he had made known to you my name. This has led me to confess that I am not as completely unknown to you as you might believe, but that fearing the ridicule attached to a female scientist I have previously taken the name of M. LeBlanc in communicating to you ... I hope that the information that I have today confided to you will not deprive me of the honor you have accorded me under a borrowed name..."

Letter from Germain to Gauss

"How can I describe my astonishment and admiration on seeing my esteemed correspondent M leBlanc metamorphosed into this celebrated person ... when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men in familiarising herself with [number theory's] knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius."

Letter from Gauss to Germain

Chapter 7

Sophie Germain–Type Criterion to Eliminate Equations

In this chapter, we appeal to classical techniques coming from algebraic number theory in order to deduce the non-existence of solutions to equations of the form:

$$ry_1^{\ell} - sy_2^{2\ell} = t$$

where ℓ is a prime, $\ell < 3 \times 10^6$. We take inspiration from the history of the Fermat equation, and in particular, the contribution of Marie–Sophie Germain.

7.1 Background: The Theorem of Sophie Germain

Since Sophie was forbidden to attend L'École Polytechnique when it opened, her main work on Fermat's Last Theorem took place through letters to Gauss and Legendre.

The Academy were awarding a prize for the proof to Fermat's Last Theorem and this renewed her interest in number theory. Correspondence with Gauss opened up once again. Reading Gauss' *Disquisitiones Arithmeticae*, Sophie had very early on made a connection between theory of *residues* and the Fermat equation.

Her initial ideas to tackle the Fermat equation can be seen in her letter to Gauss: the quotation is taken directly from [Del Centina, 2008, pg. 358–359].

> *Voici ce que j'ai trouvé:*
>
> *L'ordre dans lequel les résidus (puissances égales à l'exposant) se trouvent placés dans la série des nombres naturels détermine les diviseurs nécessaires qui appartiennent aux nombres entre lesquels on établit non*

seulement l'équation de Fermat mais encore beaucoup d'autres équations analogues à celle-là.

Prenons pour exemple l'équation même de Fermat qui est la plus simple de toutes celles dont il s'agit ici.

Soit donc, p étant un nombre premier, $z^p = x^p + y^p$. Je dis que si cette équation est possible, tout nombre premier de la forme $2Np+1$ (N tant un entier quelconque) pour lequel il n'y aura pas deux résidus) $p^{iéme}$ puissance placés de suite dans la série des nombres naturels divisera nécessairement l'un des nombres x, y et z.

Cela est évident, car l'équation $z^p = x^p + y^p$ donne la congruance [congruence] $1 \equiv r^{sp} + r^{tp}$ dans laquelle r représente une racine primitive et s et t des entiers.

On sait que l'équation a une infinité de solutions lorsque $p = 2$. Et en effet tous les nombres, exceptés 3 et 5 ont au moins deux résidus quarrés dont la différence est l'unité. Aussi dans ce cas la forme connue savoir $h^2 + f^2, 2fh, h^2 - f^2$ des nombres $z[x], y$ et z montre-t-elle que l'un de ces nombres est multiple de 3 et aussi que l'un des mêmes nombres est multiple de 5.

Il est aisé de voir que si un nombre quelconque k est résidu puissance $p^{iéme}$ mod. $2Np + 1$ et qu'il y ait deux résidus puissance $p^{iéme}$ méme mod. dont la différence soit l'unité, il y aura aussi deux résidus puissance $p^{iéme}$ dont la différence sera k.

Mais il peut arriver qu'on ait deux résidus $p^{iéme}$ dont la différence soit k, sans que k soit résidu $p^{iéme}$.

Cela posé voici l'équation générale dont la solution me semble dépendre comme celle de Fermat de l'ordre des résidus:

$$kz^p = x^p \pm y^p$$

car d'après ce que vient d'être dit on voit que tout nombre premier de la forme $2Np+1$ pour lequel deux résidus $p^{iéme}$ n'ont pas le nombre k pour différence divise le nombre z [l'un des nombres x, y, z]. Il suit delè que s'il y avait un nombre infini de tels nombres l'équation serait impossible.

There are many versions of Germain's Theorem which can be found in various books and online resources. We state her theorem in a way that I feel is closest to

her original work (which is written tersely in French), yet has been adapted to the mathematical language of today (see [Del Centina, 2008, pg. 372]).

Recall the Fermat equation:

$$x^p + y^p = z^p, \quad p \geq 3,\ p \text{ is a prime}$$

Fermat's Last Theorem can be split into two cases. The first case, often denoted FLT1, is where p does not divide x, y or z. The second case, then denoted FLT2, is when p divides one of x, y or z.

Theorem 7.1.1 (Germain)**.** *Let p be an odd prime. If there exists an auxiliary prime, $q = 2Np + 1$, where N is any integer that is not divisible by 3, such that*

1. *if $x^p + y^p + z^p \equiv 0 \pmod{q}$, then $q \mid xyz$ and*
2. *p is not a p-th power residue modulo q.*

Then, FLT1 is true for p.

Germain used this criterion to show that the Fermat equation has no solutions for all prime $p < 100$ (actually, her theorem shows that FLT1 is true for all primes $p < 197$). Many mathematicians have refined the work of Germain to prove FLT1 is true for all primes p less than some astronomical bound.

In a similar manner to Germain, by considering residue classes for our equations, we develop a criteria tailored to our equations in order to eliminate the majority of the equations when $\ell < 3 \times 10^6$.

7.2 Application: A Criterion for the Non-Existence of Solutions

In Chapter 5, we reduced the problem of solving equation (2.8) to the resolution of 906 equations of the form (5.7). In Chapter 6, we showed that the exponent ℓ is necessarily bounded by 3×10^6. In this section, we will provide a criterion for the non-existence of solutions to equation (5.7), given r, s, t and ℓ.

Lemma 7.2.1. *Let $\ell \geq 3$ be prime. Let r, s and t be positive integers satisfying $\gcd(r, s, t) = 1$. Let $q = 2k\ell + 1$ be a prime that does not divide r. Define*

$$\mu(\ell, q) = \{\eta^{2\ell} \ : \ \eta \in \mathbb{F}_q\} = \{0\} \cup \{\zeta \in \mathbb{F}_q^* \ : \ \zeta^k = 1\} \tag{7.1}$$

and

$$B(\ell, q) = \left\{ \zeta \in \mu(\ell, q) \ : \ ((s\zeta + t)/r)^{2k} \in \{0, 1\} \right\} .$$

If $B(\ell, q) = \emptyset$, then equation (5.7) does not have integral solutions.

Proof. Suppose $B(\ell, q) = \emptyset$. Let (y_1, y_2) be a solution to (5.7). Let $\zeta = \overline{y_1}^{2\ell} \in \mu(\ell, q)$. From equation (5.7) we have

$$(s\zeta + t)/r \equiv y_2^{\ell} \mod q.$$

Thus

$$((s\zeta + t)/r)^{2k} \equiv y_2^{q-1} \equiv 0 \text{ or } 1 \mod q.$$

This shows that $\zeta \in B(\ell, q)$ giving a contradiction. □

Remark: We now provide a heuristic explanation why Lemma 7.2.1 should succeed in proving the non-existence of solutions to equation (5.7), provided that there are no solutions, particularly if ℓ is large. Observe that $\#\mu(\ell, q) = k+1$. For $\zeta \in \mu(\ell, q)$, the element $((s\zeta+t)/r)^{2k} \in \mathbb{F}_q$ is either 0 or an ℓ-th root of unity. Thus the "probability" that it belongs to the set $\{0, 1\}$ is $2/(\ell + 1)$. It follows that the "expected size" of $B(\ell, q)$ is $2(k+1)/(\ell+1) \approx 2q/\ell^2$. For large ℓ we expect to find a prime $q = 2k\ell+1$ such that $2q/\ell^2$ is tiny and so we likewise expect that $\#B(\ell, q) = 0$.

7.3 Application: Elimination of 190,579,282 Equations

We wrote a `Magma` script which, for each $3 \leq d \leq 50$, and each $(\alpha, \beta) \in \mathcal{A}_d$ (and corresponding triple of coefficients (r, s, t)), and every prime $5 \leq \ell < 3 \times 10^6$, systematically searches for a prime $q = (2k\ell + 1) \nmid r$ with $k \leq 1000$ such that $B(\ell, q) = \emptyset$. If it finds such a q, then by Lemma 7.2.1 we know that equation (5.6) has no solutions, and thus there are no solutions to equation (2.8) that give rise to the pair (α, β) via Lemma 5.2.1. The entire time for the computation was roughly 3 hours on a 2500MHz AMD Opteron. The criterion systematically failed for all exponents $5 \leq \ell < 3 \times 10^6$ whenever $4\beta = d^2 - 1$ (equivalently the coefficients of equation (5.7) satisfy $r = t$). This failure is unsurprising as equations (5.6) and (5.7) have the obvious solution $(y_1, y_2) = (0, 1)$. In all cases where $4\beta \neq d^2 - 1$, the criterion succeeded for all values of ℓ except for a handful of small values. There were a total of 224 quintuples (d, ℓ, r, s, t) with $r \neq t$ for which the criterion fails. The largest value of ℓ in cases $r \neq t$ for which the criterion fails is $\ell = 19$ with $d = 27$, $\alpha = 1/7$, $\beta = 14/27$, and corresponding $r = 2744$, $s = 27$, $t = 963144$.

At this point, to complete the proof of Theorem 2.1.1, we thus require another method to handle (5.7) when $r = t$, and also some new techniques to solve this equation when $r \neq t$, for the remaining small ℓ. The first question is addressed in Chapter 8, and the second in Chapters 9 and 10.

Promise me you'll always
remember: You're braver than you
believe, and stronger than you
seem, and smarter than you think.

Winnie the Pooh, A. A. Milne

Chapter 8

The Case $r = t$: The Modular Way!

In practice, in the previous chapter, we found that Lemma 7.2.1 will eliminate all elements $(\alpha, \beta) \in \mathcal{A}_d$ for any given sufficiently large ℓ except when $\beta = (d^2-1)/4$ (which is equivalent to $r = t$). In this case, equation (5.6) has the solution $(y_1, y_2) = (0, 1)$ which causes the criterion of Lemma 7.2.1 to fail; for this situation, we would like to show that $(y_1, y_2) = (0, 1)$ is in fact the only solution.

This chapter studies the *modular approach* to solving ternary Diophantine equations. While classical techniques were incredibly useful to eliminate the majority of the equations, they are not sufficient. The *modular approach*, being a very powerful tool, is also computationally very expensive. Therefore, we do not push *all* 906 ternary equations through the modular method (although technically, one could, but one really really not ought to!)

8.1 Background: Modular Forms

This section follows Siksek's Superb Survey Article – Siksek [2012]. Another great reference is Diamond and Shurman [2005].

In this thesis, we will only consider modular forms that are cuspidal newforms of weight 2 and level $\Gamma_0(N)$. We first begin with a brief recap of some background material for newforms. We go on to state the key results that arose out of the work of Wiles et al. on Fermat's Last Theorem. These results are crucial for us as we apply them in Section 8.5.

Definition 8.1.1. *Let N be a positive integer. The modular group $\Gamma_0(N)$ is the*

group:

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \middle| \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Definition 8.1.2. *Let $\mathbb{H}$ denote the complex upper half plane. Write*

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$$

which is known as the extended upper half plane. The modular group acts on $\mathbb{H}^*$ via linear fractional transforms i.e. for $\gamma \in \Gamma_0(N)$ and for $z \in \mathbb{H}$,

$$\gamma \cdot z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty \\ \frac{a}{c} & \text{if } z = \infty \end{cases}.$$

If $c = 0$ or $cz + d = 0$, then $\gamma \cdot z = \infty$

The *cusps* of $\Gamma_0(N)$ is the set of $\Gamma_0(N)$-orbits in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

Definition 8.1.3. *A modular form of weight k and level N is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that*

1. *f is holomorphic at all cusps, and*
2. *for all $z \in \mathbb{H}$ and $\gamma \in \Gamma_0(N)$, f satisfies:*

$$f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

A modular form can be expressed as a power series (called q-expansion),

$$f(z) := \sum_{n=0}^{\infty} a_n(f) \cdot q^n, \quad \text{where } q = e^{2\pi i z}, \quad a_n(f) \in \mathbb{C}.$$

If f vanishes at all of the cusps then we call f a *cuspform*. For example, vanishing at the cusp at ∞ is equivalent to $a_0(f) = 0$. The vector space of all weight k modular forms for $\Gamma_0(N)$ is denoted by $M_k(N)$. The vector space of all weight k cuspforms for $\Gamma_0(N)$ is denoted by $S_k(N)$. $S_k(N)$ comes equipped with a Hermitian inner product, a map $\langle \cdot, \cdot \rangle : M_k(N) \times S_k(N) \mapsto \mathbb{C}$, called the Petersson inner product.

- Let M be a proper divisor of N. There are canonical maps $S_k(M) \to S_k(N)$. Let $S_k^{\mathrm{old}}(N)$ be the subspace spanned by the images of these maps for all proper divisors M of N.

- The *new subspace*, $S_k^{\text{new}}(N)$, is the orthogonal complement to $S_k^{\text{old}}(N)$ with respect to the Petersson inner-product.
- The space $S_k^{\text{new}}(N)$ is endowed with an action of commuting Hecke operators T_p and the *newforms* are a simultaneous eigenbasis for these Hecke operators.
- The Hecke eigenvalues of a newform f are equal to the coefficients of its q-expansion, $a_n(f)$, and its *Hecke eigenvalue field* is $\mathbb{Q}(a_1(f), a_2(f), \dots)$. It turns out that the latter is a number field.

Definition 8.1.4. *In the notation above, let $f(z) := \sum_{n=0}^{\infty} a_n(f) \cdot q^n$ be a newform. We say that f is rational if $a_n \in \mathbb{Q}$ for all n, otherwise we say that f is irrational.*

We will need newforms only up to *Galois conjugacy*.

Theorem 8.1.5 (Eichler–Shimura)**.** *Let f be a newform of weight 2 and level N. If f is rational, then there exists an elliptic curve, $E/\mathbb{Q}$ with conductor N such that $a_q(E) = a_q(f)$ for all primes $q \nmid N$.*

Here

$$a_q(E) = q + 1 - \#E(\mathbb{F}_q).$$

The converse of Eichler–Shimura was a conjecture for a very long time (known as the *modularity conjecture*). For any elliptic curve over the rational field, can we find a corresponding weight 2 rational newform? A positive answer to this question provides a proof to the elusive Fermat's Last Theorem. This was the final missing piece of the puzzle. Fermat's Last Theorem officially became a theorem due to Wiles et. al. The modularity conjecture was first proved by Wiles [1995] for semistable elliptic curves (i.e. ones with squarefree conductor). This specific case was enough to provide a proof for Fermat's Last Theorem. The proof of the modularity conjecture was completed in a series of papers culminating in Breuil et al. [2001].

Theorem 8.1.6 (Modularity Theorem)**.** *To any elliptic curve, $E/\mathbb{Q}$ with conductor N, we can associate a newform f of weight 2 and level N, such that for all primes $q \nmid N$, $a_q(f) = a_q(E)$.*

Together, Eichler–Shimura and the Modularity Theorem give a bijection between rational eigenforms of level N and isogeny classes of elliptic curves over the rational field of conductor N.

8.2 Background: Ribet's Level-Lowering Theorem

We continue to follow Siksek's Superb Survey Article - Siksek [2012]. Let E be an elliptic curve over $\mathbb{Q}$ given by a minimal Weierstrass model. Let f be a weight 2 newform with Hecke eigenvalue field K, and let $p \geq 5$ be a prime. We say that E is mod p congruent to f and write $E \sim_p f$ if there is a prime ideal $\varpi \mid p$ of $\mathcal{O}_K$ such that

$$a_q(E) \equiv a_q(f) \pmod{\varpi}$$

for all but finitely many primes q. In fact the following result makes this relationship more precise.

Proposition 8.2.1. *Let $E \sim_p f$ as above. Suppose E has conductor N and f has level N'. Let $q \neq p$ be a prime.*

(i) If $q \nmid NN'$ then $a_q(E) \equiv a_q(f) \pmod{\varpi}$.

(ii) If $q \nmid N'$ but $q \,||\, N$ then $q + 1 \equiv \pm a_q(f) \pmod{\varpi}$.

Note that if f is rational, then E corresponds to an elliptic curve F by Eichler–Shimura. In this case we write $E \sim_p F$ instead of $E \sim_p f$. In this case Proposition 8.2.1 maybe slightly strengthened as follows.

Proposition 8.2.2. *Suppose $E \sim_p F$ where E, F are elliptic curves over $\mathbb{Q}$ with conductors N, N'. Let q be a prime.*

(i) If $q \nmid NN'$ then $a_q(E) \equiv a_q(E) \pmod{p}$.

(ii) If $q \nmid N'$ but $q \,||\, N$ then $q + 1 \equiv \pm a_q(F) \pmod{p}$.

Proposition 8.2.2 is stronger than Proposition 8.2.1 in that it allows $q = p$.

Theorem 8.2.3 (Ribet's Level Lowering Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve in minimal model with discriminant Δ. Let N be its conductor. Let $p \geq 5$ be a prime and write*

$$N_p = \frac{N}{\prod\limits_{\substack{q \,||\, N \\ p \mid \operatorname{ord}_q(\Delta)}} q}.$$

If E does not have p-isogenies then there is a newform f of weight 2 and level N_p such that $E \sim_p f$.

In applying Ribet's Theorem we need to check for the absence of isogenies. For this we will need the following theorem of Mazur.

Theorem 8.2.4 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose that we have one of the following cases:*

- $p \geq 17$ *and* $j(E) \notin \mathbb{Z}[1/2]$,
- $p \geq 11$ *and E is semistable,*
- $p \geq 5$, $|E(\mathbb{Q})[2]| = 4$ *and E is semistable.*

Then E does not have any p-isogenies.

8.3 Background: Bounding p

We will need the following proposition which is [Siksek, 2012, Proposition 9.1]. As the proof is relatively straightforward we include it here.

Proposition 8.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let t be a divisor of the order of the torsion subgroup*[1] *of $E(\mathbb{Q})$. Let f be a weight 2 newform of level N' and let K be its Hecke eigenvalue field. Let q be a prime satisfying $q \nmid tN'$ and $q^2 \nmid N$. Write*

$$H_q := \{a \in \mathbb{Z} \ : \ q + 1 - a \equiv 0 \pmod{t}, \qquad |a| < 2\sqrt{q}\}.$$

Let

$$B_q(f) = q \cdot \mathrm{Norm}_{K/\mathbb{Q}}((q+1)^2 - a_q(f)^2) \cdot \prod_{a \in H_q} \mathrm{Norm}_{K/\mathbb{Q}}(a_q(f) - a).$$

If $p \geq 5$ is a prime for which $E \sim_p f$ then $p \mid B_q(f)$.

Proof. If $q = p$ then clearly $q \mid B_q(f)$ so we may suppose $q \neq p$. As $q^2 \nmid N$ we see that either $q \nmid N$ or $q \mid\mid N$. Suppose first that $q \mid\mid N$. By Proposition 8.2.1, part (ii), we see that $\varpi \mid (q + 1 - a_q(f))$ or $\varpi \mid (q + 1 + a_q(f))$. Thus $\varpi \mid ((q+1)^2 - a_q(f)^2)$. Since $\varpi \mid p$, taking norms we see that

$$p \mid \mathrm{Norm}_{K/\mathbb{Q}}((q+1)^2 - a_q(f)^2)$$

and so p divides $B_q(f)$.

We now suppose that $q \nmid N$. By Proposition 8.2.1, part (ii), $\varpi \mid (a - a_q(f))$ where $a = a_q(E)$ and so p divides $\mathrm{Norm}_{K/\mathbb{Q}}(a - a_q(f)$. By Hasse's bound (see

[1] We will apply this proposition to Frey curves which have unknown coefficients. We therefore do not necessarily know the torsion subgroup exactly, but we often know a subgroup of the torsion group from the form of the Frey curve.

[Silverman, 2009, Chapter 4]) $|a| < 2\sqrt{q}$. Moreover, as $q \nmid t$ and $E(\mathbb{Q})$ has a torsion subgroup of order t, we have $t \mid \#E(\mathbb{F}_q)$; this is known as the injectivity of reduction mod q map see [Silverman, 2009, Chapter 7]. But $\#E(\mathbb{F}_q) = q+1-a$. Thus $a \in H_q$. Hence p divides

$$\prod_{a \in H_q} \text{Norm}_{K/\mathbb{Q}}(a - a_q(f)).$$

So $p \mid B_q(f)$. □

8.4 Background: Modular Cooking – Recipe for Signature (p, p, p)

In the previous section, we saw the key theorems that went into Wiles' proof of Fermat's Last Theorem. Now that we have an incredibly powerful tool, how do we *actually* use it? Most importantly for us: how can we use this shiny new gadget to solve our consecutive cubes conundrum?

Siksek's Superb Survey Article - Siksek [2012], gives a crystal clear exposition which shows the practical *hands–on–approach* to solving Diophantine equations using the modular method. So of course, we will follow Siksek's Superb Survey Article - Siksek [2012].

Definition 8.4.1. *A ternary Diophantine equation is of the form*

$$Ax^p + By^q = Cz^r \tag{8.1}$$

where p, q and r are non-zero positive integers such that $1/p + 1/q + 1/r < 1$. The signature of a ternary Diophantine equation is given by the tuple (p, q, r).

The reason we impose the condition $1/p + 1/q + 1/r < 1$ is related to the Beal Conjecture and Fermat–Catalan equation:

Conjecture 8.4.2 (Beal)**.** *The equation*

$$x^p + y^q = z^r, \qquad p,\ q,\ r \in \mathbb{Z}, \quad p,\ q,\ r > 2$$

with x, y, z pairwise coprime has no integer solutions.

Andrew Beal, in 1993, a banker with a wider interest in Number Theory and in particular, the generalised Fermat equation, has offered a monetary reward for the solution of this conjecture. Apparently, the prize money has increased several times already, and is currently worth around one million dollars! In other literature,

the conjecture has also been referred to as the generalized Fermat equation, the Mauldin conjecture and the Tijdeman–Zagier conjecture.

Conjecture 8.4.3 (Fermat-Catalan)**.** *The equation*

$$x^p + y^q = z^r, \qquad p,\ q,\ r \in \mathbb{N},$$

with x, y, z pairwise coprime and p, q, r such that $1/p + 1/q + 1/r < 1$. has only finitely many solutions.

Beal's Conjecture can now be seen as equivalent to the Fermat-Catalan equation only having solutions when one of p, q, r is equal to 2.

Remark: If $p = q = r = 2$, then equation (8.1) has infinitely many solutions. A classical example is to let $A = B = C = 1$. Then Pythagoras' Theorem gives us infinitely many integer solutions to $x^2 + y^2 = z^2$.

In Chapter 5, after a little algebraic manipulation of our equation, we are reduced to solving many ternary Diophantine equations with signature (p, p, p). Kraus [1997] gives a recipe to determine the associated Frey-Hellegouarch curve, with the corresponding invariants, as well as determining explicitly the space of newforms, giving the weight and the level.

We consider the ternary Diophantine equation of signature (p, p, p),

$$Ax^p + By^p = Cz^p \qquad p \geq 5. \tag{8.2}$$

The Assumptions (Without Loss of Generality):

- We suppose that A, B and C are non-zero integers and pairwise coprime.[2]
- We suppose that p is prime.[3]
- We let $R = ABC$. We can assume that $\mathrm{ord}_q(R) < p$, for every prime q.[4]
- We assume that Ax, By and Cz are pairwise coprime.

[2] If they are not pairwise coprime, then one can always divide by the greatest common divisor.

[3] If p is not prime, then we can always factorise the exponent and absorb the excess factors into the variables x, y and z, leaving us with a prime exponent. When the factors of the exponent are only 2 and/or 3 then we must use an alternative method to solve the equation, for example, as seen in Chapter 3 which uses elliptic curves for the case $p = 2$ and Chapter 10 which uses a Thue Solver in `Magma` to solve equations when $p = 3$.

[4] If not, then at least one of A, B, C has a $p-$th power as a factor. Given the equation, we may absorb any excess p-th powers into the appropriate variable x, y, z.

- We assume $By^p \equiv 0 \pmod 2$.[5]
- We assume $Ax^p \equiv -1 \pmod 4$.[6]

To equation 8.2, we attach the Frey–Hellegouarch curve,

$$E := Y^2 = X(X - Ax^p)(X + By^p).$$

The minimal discriminant is given by

$$\Delta = \begin{cases} 2^4 R^2 (xyz)^{2p} & \text{if } 16 \nmid By^p, \\ 2^{-8} R^2 (xyz)^{2p} & \text{if } 16 \mid By^p. \end{cases}$$

For a positive integer M, we denote by $\mathrm{Rad}(M)$ the product of all primes dividing M; this is known as the *radical* of M. We also write $\mathrm{Rad}_2(M)$ for the product of all odd primes dividing M. For example, $150 = 2 \times 3 \times 5^2$ which gives us $\mathrm{Rad}(150) = 30$ and $\mathrm{Rad}_2(150) = 15$.

The conductor of E is given by

$$N = \begin{cases} 2\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 0 \text{ or } \mathrm{ord}_2(R) \geq 5, \\ 2\,\mathrm{Rad}_2(Rxyz) & \text{if } 1 \leq \mathrm{ord}_2(R) \leq 4 \text{ and } y \text{ is even}, \\ \mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 4 \text{ and } y \text{ is odd}, \\ 2^3\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 2 \text{ or } 3 \text{ and } y \text{ is odd}, \\ 2^5\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 1 \text{ and } y \text{ is odd}. \end{cases}$$

Theorem 8.4.4 (Kraus [1997])**.** *Suppose $p \geq 5$. With the above assumptions and notation, $E \sim_p f$ for a newform f of level given by*

$$N_p = \begin{cases} 2\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 0 \textit{ or } \mathrm{ord}_2(R) \geq 5, \\ \mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 4, \\ 2\,\mathrm{Rad}_2(R) & \textit{if } 1 \leq \mathrm{ord}_2(R) \leq 3 \textit{ and } y \textit{ is even}, \\ 2^3\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 2 \textit{ or } 3 \textit{ and } y \textit{ is odd}, \\ 2^5\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 1 \textit{ and } y \textit{ is odd}. \end{cases}$$

[5] Suppose $Ax^p, By^p, Cz^p \equiv 1 \pmod 2$. Looking at equation (8.2) modulo 2, we arrive at a contradiction. Hence one of Ax^p, By^p, Cz^p is congruent to 0 (mod 2), and only one, otherwise we would contradict our pairwise coprimality assumption.

[6] $Ax^p \not\equiv 0, 2 \pmod 4$ since then it would contradict gcd conditions. If $Ax^p \equiv -1 \pmod 4$ then we are done. If not, then we are in the case $Ax^p \equiv 1 \pmod 4$. We may simply multiply equation (8.2) by -1 to obtain the desired result.

Kraus's Theorem is in essence a corollary of Ribet's Theorem. Kraus explicitly calculates the minimal discriminant and conductor of the Frey curve E and writes down N_p.

8.5 Application: Frey-Hellegouarch Curve for the Case $r = t$

In practice, we found that Lemma 7.2.1 will eliminate all elements $(\alpha, \beta) \in \mathcal{A}_d$ for any given sufficiently large ℓ except when $\beta = (d^2-1)/4$ (which is equivalent to $r = t$). In this case, equation (5.6) has the solution $(y_1, y_2) = (0, 1)$ which causes the criterion of Lemma 7.2.1 to fail; for this situation, we would like to show that $(y_1, y_2) = (0, 1)$ is in fact the only solution. In this section, we will thus focus on equation (5.6) for $\beta = (d^2-1)/4$, and continue to suppose that $\ell \geq 5$ is prime. It follows from the definition of $\mathcal{A}_d$ that $\alpha = 8/d(d^2-1)$, and moreover that this pair $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/4)$ arises exactly when either $\mathrm{ord}_2(d) = 0$ or 3. We can rewrite (5.6) as

$$y_2^\ell - \frac{64}{d^2(d^2-1)^3} \cdot y_1^{2\ell} = 1. \tag{8.3}$$

We note from equation (5.2) that y_1 is even if $\mathrm{ord}_2(d) = 0$ and y_1 is odd if $\mathrm{ord}_2(d) = 3$. By the conclusion of Lemma 5.2.1, we know that y_1 and y_2 are integers. It follows from equation (8.3) that $S \mid y_1$ where

$$\begin{cases} S = \mathrm{Rad}\left(d(d^2-1)\right) & \text{if } \mathrm{ord}_2(d) = 0, \\ S = \mathrm{Rad}_2\left(d(d^2-1)\right)\right) & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

Let $y_1 = Sy_3$. Then, from equation (8.3),

$$y_2^\ell - Ty_3^{2\ell} = 1 \tag{8.4}$$

where

$$T = \frac{64S^{2\ell}}{d^2(d^2-1)^3}.$$

In addition to the assumption $\ell \geq 5$, let us further suppose that

$$2\ell > \mathrm{ord}_q(d^2(d^2-1)^3) \tag{8.5}$$

for all odd primes q. If $\mathrm{ord}_2(d) = 0$, we will also assume that

$$2\ell \geq 3\,\mathrm{ord}_2(d^2-1) - 1. \tag{8.6}$$

From assumptions (8.5) and (8.6), it follows that T is an integer and that $\mathrm{Rad}(T) = S$. If $\mathrm{ord}_2(d) = 0$, then $2^5 \mid T$. If, however, $\mathrm{ord}_2(d) = 3$, then $\mathrm{ord}_2(T) = 0$ and $2 \nmid y_3 \mid y_1$ so that $2 \mid y_2$. We would like to show that all solutions to (8.3) satisfy $y_1 = 0$, so suppose $y_1 \neq 0$ (which implies $y_3 \neq 0$). Clearly $y_2 \neq 0$. Following the recipe of Kraus given in Section 8.4 we associate to our solution (y_2, y_3) the Frey–Hellegouarch curve

$$\begin{cases} E \ : \ Y^2 = X(X+1)(X - Ty_3^{2\ell}) & \text{if } \mathrm{ord}_2(d) = 0, \\ E \ : \ Y^2 = X(X+1)(X + y_2^{\ell}) & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

Again, using the recipe, the minimal discriminant and conductor of E are

$$\Delta = 2^{-8} T^2 y_2^{2\ell} y_3^{4\ell}, \qquad N = 2\,\mathrm{Rad}_2(T y_2 y_3). \tag{8.7}$$

Thus $E \sim_\ell f$ where f is a weight 2 newform of level $N_\ell = 2\,\mathrm{Rad}_2(T)$. Recall that $\mathrm{Rad}(T) = S$. Moreover T is odd if and only if $\mathrm{ord}_2(d) = 3$. Thus

$$N_\ell = \begin{cases} S & \text{if } \mathrm{ord}_2(d) = 0 \\ 2S & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

We can now apply Proposition 8.3.1. Since E has full 2-torsion, we take $t = 4$ in the statement of that proposition. Let $q \nmid N_\ell$ be an odd prime. From (8.7) we see that $q^2 \nmid N$ (since Rad_2 is always squarefree). Thus $\ell \mid B_q(f)$. If $B_q(f) \neq 0$ then we have obtained a bound for ℓ. Note from the formula for $B_q(f)$, if $a_q(f)$ is irrational, then the differences $a - a_q(f)$ are non-zero for $a \in H_q$ (the a are integers). Moreover the factor $(q+1)^2 - a_q(f)$ is also non-zero since $|a_q(f)| < 2\sqrt{q}$. In this case $B_q(f) \neq 0$. In fact if the newform f is irrational then there is a positive density of q such that $a_q(f)$ is irrational (see Siksek [2012]), thus we certainly obtain a bound on ℓ. We can usually improve on this bound by choosing a set of odd primes $\mathcal{Q} = \{q_1, \ldots, q_n\}$ all not dividing N_ℓ and letting

$$B_{\mathcal{Q}}(f) = \gcd(B_q(f) \ : \ q \in \mathcal{Q}).$$

If $E \sim_\ell f$ then $\ell \mid B_{\mathcal{Q}}(f)$. Unfortunately if f is a rational newform (hence corresponding to some elliptic curve E') then $B_q(f)$ is very often zero and sometimes always zero. See Siksek's Superb Survey Article - Siksek [2012] for examples.

Lemma 8.5.1. *Let $3 \leq d \leq 50$ with $\mathrm{ord}_2(d) = 0$ or 3. Suppose $\ell \geq 5$ is a prime that satisfies* (8.5) *for all odd primes q. If $\mathrm{ord}_2(d) = 0$, suppose ℓ also satisfies* (8.6)*. Let*

N_ℓ be as above. Suppose for each irrational newform of weight 2 and level N there is a set of primes $\mathcal{Q}$ not dividing N such that $\ell \nmid B_{\mathcal{Q}}(f)$. Suppose for every elliptic curve F of conductor N_ℓ there is a prime $q = 2k\ell + 1$, $q \nmid N_\ell$, such that

(i) $B(\ell, q) = \{\overline{0}\}$, where $B(\ell, q)$ is as in the statement of Lemma 7.2.1;

(ii) $\ell \nmid (a_q(F)^2 - 4)$.

Then

- *if $\mathrm{ord}_2(d) = 3$ then (2.8) has no solutions with $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ in Lemma 5.2.1;*
- *if $\mathrm{ord}_2(d) = 0$ then the only solution to (2.8) with $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ in Lemma 5.2.1 satisfies $x = -(d+1)/2$.*

Proof. The conclusion of the lemma is immediate if $y_1 = 0$ in (5.2). Let us thus suppose that $y_1 \neq 0$ and attempt to deduce a contradiction. From the above discussion, there is a newform f of level N_ℓ such that $E \sim_\ell f$, where E is the Frey–Hellegouarch curve. If f is irrational then $\ell \mid B_{\mathcal{Q}}(f)$, which contradicts the hypotheses of the lemma. Thus f is rational and so by Eichler–Shimura f corresponds to an elliptic curve $F/\mathbb{Q}$ of conductor N. Thus $E \sim_\ell F$.

Suppose (i). By the proof of Lemma 7.2.1 we have that $q \mid y_1$. Thus $q \mid y_3$. By (8.7) we see that $q \mid\mid N$. Thus by Proposition 8.2.2 we have $(q+1) \equiv \pm a_q(F) \mod \ell$. As $q \equiv 1 \mod \ell$ we obtain $4 \equiv a_q(F)^2 \mod \ell$. This contradicts (ii) and completes the proof. □

Remark: In this section, we are concerned with equation (5.6) with $4\beta = d^2 - 1$, or equivalently equation (5.7) with $r = t$. These have the solution $(y_1, y_2) = (0, 1)$. It follows from the proof of Lemma 7.2.1 that $\overline{0} \in B(\ell, q)$ (for any suitable q) and thus $B(\ell, q) \neq \emptyset$. However, in this case, the heuristic remark following the proof of Lemma 7.2.1 leads us to expect $B(\ell, q) = \{\overline{0}\}$ for sufficiently large ℓ (and suitable q).

8.5.1 Proof of Theorem 2.1.1: The Case $r = t$

We wrote a `Magma` script which, for each $3 \leq d \leq 50$ with $\mathrm{ord}_2(d) = 0$ or 3, computes the newforms of weight 2, level N_ℓ. Our script takes $\mathcal{Q}$ to be the set of primes < 100 that do not divide N_ℓ, and computes $B_{\mathcal{Q}}(f)$ for each irrational eigenform f at level N_ℓ. These unsurprisingly are all non-zero. For every prime $5 \leq \ell < 3 \times 10^6$ that does not divide any of the $B_{\mathcal{Q}}(f)$, and satisfies inequality (8.5), and also inequality (8.6)

if $\mathrm{ord}_2(d) = 0$, and for every isogeny class of elliptic curves F of conductor N_ℓ, the script systematically searches for a prime $q = (2k\ell + 1) \nmid r$ with $k \leq 1000$ such that conditions (i) and (ii) of Lemma 8.5.1 hold. If it finds such a q we know that there are no solutions to (2.8) that give rise to the pair $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ via Lemma 8.5.1. The entire time for the computation was roughly 2.5 hours on a 2500MHz AMD Opteron. In all cases the criterion succeeded for all values of ℓ except for a handful of small values. There were a total of 53 quintuples (d, ℓ, r, s, t) with $r = t$ for which either ℓ does not satisfy the inequalities (8.5), (8.6), or it divides $B_{\mathcal{Q}}(f)$ for some irrational eigenform, or for which the script did not find a suitable q that satisfies (i), (ii). The largest value of ℓ among the 53 quintuples is $\ell = 19$: with $d = 37$, $r = t = 54762310872$, $s = 1$, and with $d = 40$, $r = t = 102208119975$, $s = 1$.

"I'm so tired my tired is tired..."

Winnie the Pooh, A. A. Milne

Chapter 9

Eliminating More Equations

Looking back at Sections 5.4, 7.3 and 8.5.1, we see that in order to complete the proof of Theorem 2.1.1, we need to solve $224 + 53 + 942 = 1219$ equations of the form (5.7), with r, s and t positive integers and $\gcd(r, s, t) = 1$. In the second column of Table 9.1 we give a breakdown of these equations according to the exponent ℓ. In what follows we look at two methods to eliminate most of these equations, and one method for solving the remaining 226 equations.

Exponent ℓ	original number of equations (5.7) with exponent ℓ	number surviving after local solubility tests	number surviving after further descent
3	942	393	223
5	179	63	3
7	77	35	0
11	10	7	0
13	5	4	0
17	3	2	0
19	3	3	0
Total	1219	507	226

Table 9.1: In Sections 7.3, 8.5.1 and 5.4, we have reduced the proof of Theorem 2.1.1 to the resolution of 1219 equations of the form (5.7). The first and second columns give a breakdown of this number according to the exponent ℓ. The third column gives the number of these equations surviving the local solubility tests of Section 9.1, and the fourth column gives the number that then survive the further descent of Section 9.2.

9.1 Local Solubility

Recall that $\gcd(r,s,t) = 1$ in (5.7). Write $g = \mathrm{Rad}(\gcd(r,t))$ and suppose that $g > 1$. Then $g \mid y_1$, and we can write $y_1 = gy_1'$, and thus

$$ry_2^\ell - sg^{2\ell}{y_1'}^{2\ell} = t.$$

Now we may remove a factor of g from the coefficients to obtain

$$r'{y_2}^\ell - s'{y_1'}^{2\ell} = t',$$

where $t' = t/g < t$. Likewise, if $h = \gcd(s,t) > 1$, we obtain an equation

$$r'{y_2'}^\ell - s'{y_1}^{2\ell} = t',$$

Likewise where $t' = t/h < t$. We apply these operations repeatedly until we arrive at an equation of the form

$$R\rho^\ell - S\sigma^{2\ell} = T \tag{9.1}$$

where R, S, T are pairwise coprime. A necessary condition for the existence of solutions is that for any odd prime $q \mid R$, the residue $-ST$ modulo q is a square. Besides this simple test we check for local solubility at the primes dividing R, S, T, and the primes $q \leq 19$. We subjected all of the 1219 equations to these local solubility tests. These have allowed us to eliminate 712 equations, leaving 507 equations. A breakdown of these according to the exponent ℓ is given in the third column of Table 9.1.

9.2 A Further Descent

If local solubility fails to rule out solutions then we carry out a descent to do so. Specifically, let

$$S' = \prod_{\mathrm{ord}_q(S) \text{ is odd}} q.$$

Thus $SS' = v^2$. Write $RS' = u$ and $TS' = mn^2$ with m squarefree. We may now rewrite (9.1) as

$$(v\sigma^\ell + n\sqrt{-m})(v\sigma^\ell - n\sqrt{-m}) = u\rho^\ell.$$

Let $K = \mathbb{Q}(\sqrt{-m})$ and $\mathcal{O}$ be its ring of integers. Let $\mathfrak{S}$ be the prime ideals of $\mathcal{O}$ that divide u or $2n\sqrt{-m}$. Clearly $(v\sigma^\ell + n\sqrt{-m})K^{*\ell}$ belongs to the "ℓ-Selmer group"

$$K(\mathfrak{S}, \ell) = \{\epsilon \in K^*/K^{*\ell} \ : \ \mathrm{ord}_{\mathcal{P}}(\epsilon) \equiv 0 \mod \ell \text{ for all } \mathcal{P} \notin \mathfrak{S}\}.$$

This is an $\mathbb{F}_\ell$-vector space of finite dimension and, for a given ℓ [Silverman, 2009, Proof of Proposition VIII.1.6]), it can be computed by `Magma` using the command `pSelmerGroup`. Let

$$\mathcal{E} = \{\epsilon \in K(\mathfrak{S}, \ell) \ : \ \mathrm{Norm}(\epsilon)/u \in \mathbb{Q}^{*\ell}\}.$$

It follows that

$$v\sigma^\ell + n\sqrt{-m} = \epsilon\eta^\ell, \tag{9.2}$$

where $\eta \in K^*$ and $\epsilon \in \mathcal{E}$.

Lemma 9.2.1. *Let $\mathfrak{q}$ be a prime ideal of K. Suppose one of the following holds:*

(i) $\mathrm{ord}_{\mathfrak{q}}(v)$, $\mathrm{ord}_{\mathfrak{q}}(n\sqrt{-m})$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$ *are pairwise distinct modulo ℓ;*

(ii) $\mathrm{ord}_{\mathfrak{q}}(2v)$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$, $\mathrm{ord}_{\mathfrak{q}}(\overline{\epsilon})$ *are pairwise distinct modulo ℓ;*

(iii) $\mathrm{ord}_{\mathfrak{q}}(2n\sqrt{-m})$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$, $\mathrm{ord}_{\mathfrak{q}}(\overline{\epsilon})$ *are pairwise distinct modulo ℓ.*

Then there is no $\sigma \in \mathbb{Z}$ and $\eta \in K$ satisfying (9.2).

Proof. Suppose (i) holds. Then the three terms in (9.2) have pairwise distinct valuations, so (9.2) is impossible $\mathfrak{q}$-adically. If (ii) or (iii), then we apply the same idea to

$$2v\sigma^\ell = \epsilon\,\eta^\ell + \overline{\epsilon}\,\overline{\eta}^\ell, \qquad 2n\sqrt{-m} = \epsilon\,\eta^\ell - \overline{\epsilon}\,\overline{\eta}^\ell\,,$$

which follow from (9.2), and its conjugate equation. □

Lemma 9.2.2. *Let $q = 2k\ell + 1$ be a prime. Suppose $q\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{q}_1$, $\mathfrak{q}_2$ are distinct, and such that* $\mathrm{ord}_{\mathfrak{q}_j}(\epsilon) = 0$ *for $j = 1, 2$. Let*

$$\chi(\ell, q) = \{\eta^\ell \ : \ \eta \in \mathbb{F}_q\}.$$

Let

$$C(\ell, q) = \{\zeta \in \chi(\ell, q) \ : \ ((v\zeta + n\sqrt{-m})/\epsilon)^{2k} \equiv 0 \text{ or } 1 \mod \mathfrak{q}_j \text{ for } j = 1, 2\}.$$

Suppose $C(\ell, q) = \emptyset$. Then there is no $\sigma \in \mathbb{Z}$ and $\eta \in K$ satisfying (9.2).

Proof. The proof is a straightforward modification of the proof of Lemma 7.2.1. □

We have found Lemmata 9.2.1 and 9.2.2 useful in eliminating many, and often all, $\epsilon \in \mathcal{E}$. Of course if they succeed in eliminating all $\epsilon \in \mathcal{E}$ then we know that equation (9.1) has no solutions, and so the same would be true for equation (5.7). Of course, when $r = t$, equation (5.7) always has a solution, namely $(y_1, y_2) = (0, 1)$. For $r = t$, the reduction process in Section 9.1 leads to equation (9.1) with $R = T = 1$. The solution $(y_1, y_2) = (0, 1)$ to (5.7) corresponds to the solution $(\rho, \sigma) = (1, 0)$ in equation (9.1). It follows from equation (9.2) that $n\sqrt{-m}K^{*\ell} \in \mathcal{E}$. Naturally, Lemma 9.2.1 and Lemma 9.2.2 do not eliminate the case $\epsilon = n\sqrt{-m}$ since equation (9.2) has the solution with $\sigma = 0$ and $\eta = 1$. In this case, our interest is in showing that this is the only solution.

Lemma 9.2.3. *Suppose*

(i) $\mathrm{ord}_{\mathfrak{q}}(n\sqrt{-m}) < \ell$ *for all prime ideals* $\mathfrak{q}$ *of* $\mathcal{O}$*;*

(ii) the polynomial $X^\ell + (d - X)^\ell - 2$ *has no roots in* $\mathcal{O}$ *for* $d = 1, -1, -2$*;*

(iii) the only root of the polynomial $X^\ell + (2 - X)^\ell - 2$ *in* $\mathcal{O}$ *is* $X = 1$*.*

Then, for $\epsilon = n\sqrt{-m}$*, the only solution to* (9.2) *with* $\sigma \in \mathbb{Z}$ *and* $\eta \in K$ *is* $\sigma = 0$ *and* $\eta = 1$*.*

Proof. Let $\epsilon = n\sqrt{-m}$ and suppose $\sigma \in \mathbb{Z}$ and $\eta \in K$ is a solution to (9.2). Note that the left-hand side of (9.2) belongs to $\mathcal{O}$, and from (i), we deduce that $\eta \in \mathcal{O}$. Now subtracting (9.2) from its conjugate and dividing by $n\sqrt{-m}$ leads to the equation

$$\eta^\ell + \overline{\eta}^\ell = 2.$$

We deduce that the rational integer $\eta + \overline{\eta}$ divides 2 and hence $\eta + \overline{\eta} = d$ where $d = \pm 1, \pm 2$. Thus η is a root of $X^\ell + (d - X)^\ell - 2$ for one of these values of d. By (ii), (iii) it follows that $d = 2$ and $\eta = 1$. From (9.2) we see that $\sigma = 0$. □

For each of the 507 equations (5.7) that survive the local solubility tests in Section 9.1, we computed the set $\mathcal{E}$ and applied the criteria in Lemma 9.2.1 and Lemma 9.2.2 (the latter with $k \leq 1000$) to eliminate as many of the $\epsilon \in \mathcal{E}$ as possible. If the two lemmata succeed in eliminating all possible values of ϵ then (9.1) has no solutions, and therefore equation (5.7) does not have solutions either. If they succeeded in eliminating all but one value $\epsilon \in \mathcal{E}$, and that value is $n\sqrt{-m}$, then we checked the conditions of Lemma 9.2.3 which if satisfied allow us to conclude that

$\sigma = 0$ and therefore $y_1 = 0$. Recall that Theorem 2.1.1 is concerned with (2.8) with $x \geq 1$. If $y_1 = 0$ then $x = -(d+1)/2$ (via (5.2)) and so we can eliminate (r, s, t) if Lemmata 9.2.1, 9.2.2 and 9.2.3 allow us to conclude that $\sigma = 0$. Using this method, we managed to eliminate 281 of the 507 equations (5.7), leaving just 226 equations. In Table 9.1 we provide a breakdown of these according to the the exponent ℓ.

When we asked Pooh what the opposite of an Introduction was, he said "The what of a what?" which didn't help us as much as we had hoped, but luckily Owl kept his head and told us that the Opposite of an Introduction, my dear Pooh, was a Contradiction; and, as he is very good at long words, I am sure that that's what it is.

Winnie the Pooh, A. A. Milne

Chapter 10

A Thue Approach

Now that we have whittled our approximately two million equations down to a mere 226 equations, we are ready to solve them and determine all of their solutions. For this, we use `Magma's` Thue Solver. As usual, we first provide some background on the methodology, and then the final application to our sums of consecutive cubes.

10.1 Background: Thue Equations

We recommend the treatment in Smart [1998]. A Thue equation is a Diophantine equation of the form

$$f(x, y) = m \tag{10.1}$$

where $f(x, y)$ is a homogeneous[1] polynomial of degree at least 3 with integer coefficients and m is a fixed integer. We would like to determine all of the integer solutions (x, y) to equation (10.1). Note that we may assume that f is irreducible: the case of f being reducible follows easily from the irreducible case.

Reminiscent[2] of Chapter 3, our discussions once again turn to effective and ineffective computational methods and proof.

Theorem 10.1.1 (Axel Thue 1909)**.** *Thue equations have finitely many integer solutions in* (x, y)*.*

Thue's proof is ineffective - and once again, it was due to Baker's pioneering work on linear forms in logarithms in the late 1960s that gives us effective methods and provides a finite search region. Baker bounds are explicitly dependent on the

[1] This means that each non-zero term has the same degree. In this case it is the total degree of x and y since we are in two variables.

[2] What feels like the end is often the beginning...

coefficients of $f(x, y)$ and on m - hence effective. Baker's theory provides exceptionally large bounds, as we saw earlier, which are impractical for any computer search! This has in turn lead to decades of work on reducing the bounds. Once again, the LLL algorithm can be used to considerably reduce the size of these bounds, and the combination of these two very powerful approaches provides a practical resolution of Thue equations, provided that the degree, the coefficients and m are not too large. Fortunately for us, this method, which is explained in great detail in Smart [1998], is already implemented in `Magma` and we can simply apply it as a black box.

10.2 Application: Finding the Final Solutions!

Finally, writing $\tau = \sigma^2$ in equation (9.1), we obtain the (binomial) Thue equation:

$$R\rho^\ell - S\tau^\ell = T.$$

We solved the remaining 226 equations using the Thue equation solver in `Magma`. The theory behind this Thue equation solver is discussed in [Smart, 1998, Chapter VII]. As we see from Table 9.1, we are left with the problem of solving 223 Thue equations of degree 3, and three Thue equations of degree 5. Working backwards from these solutions, we obtained precisely six solutions to (2.8) with $x \geq 1$. These are

$$3^3 + 4^3 + 5^3 = 6^3, \qquad 11^3 + 12^3 + 13^3 + 14^3 = 20^3,$$
$$3^3 + 4^3 + 5^3 + \cdots + 22^3 = 40^3,$$
$$15^3 + 16^3 + 17^3 + \cdots + 34^3 = 70^3,$$
$$6^3 + 7^3 + 8^3 + \cdots + 30^3 = 60^3,$$
$$291^3 + 292^3 + 293^3 + \cdots + 339^3 = 1155^3.$$

Noting that these solutions are in Table 2.1, this finally completes the proof of Theorem 2.1.1.

Part II

Perfect Powers that are Sums of Consecutive like Powers

"Before beginning a Hunt,
it is wise to ask someone
what you are looking for
before you begin looking for it."

Winnie the Pooh, A. A. Milne

Chapter 11

Introduction

In Part I of this thesis, we considered the equation

$$(x+1)^k+(x+2)^k+\cdots+(x+d)^k = y^n, \qquad x,\ y,\ n,\ d,\ k \in \mathbb{Z}, \qquad d,\ k,\ n \geq 2, \quad (11.1)$$

and we found all integer solutions (x, y, n), when $k = 3$ and $2 \leq d \leq 50$. 'Complicated' Diophantine equations have rather few solutions and it was surprising that we unearthed five brand new non-trivial solutions when $n = 3$. Indeed, when $k = 2$ or $k = 4$, a computer search for integer solutions to equation (11.1) for various values of d produced no solutions. In this part of the thesis, I provide a rigorous formulation and proof for this vague "feeling that there are no solutions" in the case when k is any positive even integer. This is my version of the published joint paper Patel and Siksek [2017].

The case $k = 2$ was studied by Zhang and Bai [2013]. When $k = 2$, they show that if q is a prime congruent to $\pm 5 \pmod{12}$ and $\mathrm{ord}_q(d) = 1$, then equation (11.1) has no integer solutions (x, y, n). It follows from a standard result in analytic number theory (Dirichlet's theorem, see Theorem 11.1.2) that the set of d for which there is an integer solution with $k = 2$ has natural density 0.

11.1 Motivation: The Case $k = 2$

Before diving into the mathematics, we first investigate the case $k = 2$ and study the main objects at play. The aim of this section is twofold: firstly, the case $k = 2$ provides a simple example to motivate the generalisation to all positive even integers k and secondly, gives insight towards a possible proof for any even value of k. Just as in Part I of this thesis, don't worry if some of the terms are not immediately understandable - I will try to give a high level overview of these concepts without

assuming too much background knowledge within the *Background* sections of each subsequent chapter. If the terms are completely comprehensible, then please feel free to omit the *Background* sections.

Let's consider a slight modification to the equation that we are used to seeing.

$$x^k+(x+1)^k+\cdots+(x+d-1)^k = y^n, \qquad x,\ y,\ n,\ d,\ k \in \mathbb{Z}, \qquad d,\ k,\ n \geq 2. \tag{11.2}$$

The shift in x simply declutters the proofs in this part of the thesis. Let $k = 2$ in equation (11.2). Then we obtain the equation:

$$x^2 + (x+1)^2 + \cdots + (x+d-1)^2 = y^n. \tag{11.3}$$

Expanding and factorising the left hand side gives us the following equation:

$$d\left(x^2 + (d-1)x + \frac{(d-1)(2d-1)}{6}\right) = y^n. \tag{11.4}$$

The idea

Let $q \neq 2$ or 3 be a prime dividing d exactly once, usually denoted by $q \parallel d$. Clearly q divides the left-hand side of equation (11.4). Therefore q must divide the right-hand side. However, on the right hand side we have a number that is an n-th power. Therefore q must divide the right hand side at least n times. We then take this idea back to the left hand side: q must divide the expression in brackets at least $n-1$ times. However, if q does not divide the expression in brackets, then we can conclude that $n = 1$: q divides the left-hand side only once, therefore it can only divide the right-hand side once. In mathematical terms, we are checking that the *valuation* of a prime dividing d are the same on both sides of the equation.

Reduction Modulo q

Let q be a prime not equal to 2 or 3 such that $q \parallel d$. Suppose that q divides $(x^2 + (d-1)x + (d-1)(2d-1)/6)$. Then we obtain the congruence equation:

$$x^2 - x + 1/6 \equiv 0 \pmod{q}.$$

By completing the square, we get:

$$(x - 1/2)^2 \equiv 1/12 \pmod{q},$$

which is equivalent to:

$$(6x-3)^2 \equiv 3 \pmod{q}.$$

Thus 3 is a square modulo q. By the *Law of Quadratic Reciprocity*, it follows that $q \equiv \pm 1 \pmod{12}$.

We have now proved the theorem of Zhang and Bai [2013].

Theorem 11.1.1 (Zhang and Bai)**.** *Let $d \geq 2$ be an integer. Let q be a prime such that $q \equiv \pm 5 \pmod{12}$. Suppose $q \parallel d$. Then the equation $x^2 + (x+1)^2 + \cdots + (x+d-1)^2 = y^n$ has no integer solutions with $n \geq 2$.*

Further Questions

How many primes are there in the congruence class $\pm 5 \pmod{12}$? Are there infinitely many? If there are infinitely many, then we have infinitely many values of d such that equation (11.3) has no integer solution. What does this set of d look like, i.e. can we compare it to the set of natural numbers?

We are able to answer the first question immediately: there are infinitely many primes in the congruence class $\pm 5 \pmod{12}$. This is due to a well-known theorem of Dirichlet (see for example [Murty, 2008, Section 2.3]).

Theorem 11.1.2 (Dirichlet)**.** *Let a and n be coprime integers. Then there exists infinitely many primes, $\{p_i\}$ such that $p_i \equiv a \pmod{n}$. Moreover,*

$$\sum p_i^{-1} = \infty.$$

To say something about the set of d's we need to use Niven's theorem. The setup and details for Niven's theorem can be found in Chapter 13. Niven's theorem tells us that the set of d where there are no solutions to equation (11.3) is very dense in the positive natural numbers. In fact it has density 1. Niven's theorem tells us that if we choose a positive number d at random, then there is 0% chance of equation (11.3) having a solution. This does not mean that there is *never* a solution, just the chances of having a solution are extremely slim. We have mathematically justified our "feeling of nothingness" in the case $k = 2$.

Other values of k?

If $k = 4$, then we can follow the steps outlined above almost exactly (change a few of the numbers and Hey Presto!) and arrive at the same density conclusion. However, the reader and keen equation solver may have noticed that when $k = 6$, everything falls apart pretty quickly. There are two main hindrances here: quadratic reciprocity no longer applies when $k \geq 6$ to give us a precise congruence class to then apply Dirichlet's Theorem.

Hope: Do not despair my dear readers, not all is lost! Instead of Dirichlet's theorem, we can appeal to Chebotarev's theorem! We will need the correct setup in order to use Chebotarev's results.

11.2 The Results

Recall the equation:

$$x^k+(x+1)^k+\cdots+(x+d-1)^k = y^n, \qquad x,\ y,\ n,\ d,\ k \in \mathbb{Z}, \qquad d,\ k,\ n \geq 2. \quad (11.5)$$

In this part of the thesis, we want to show that the results found for the case $k = 2$ are also true for any positive even integer k. So, let k be a positive even integer. We rigorously show that if we choose an integer d at random from the set of natural numbers, then there is 100% chance that equation (11.5) has no integer solutions. This perfectly encapsulates the "feeling of nothingness".

The theorem below is a mathematical translation of "it is extremely very likely that these equations do not have integer solutions". We actually obtain density results for perfect powers that are sums of like powers in any arithmetic progression.

Theorem 11.2.1. *Let $k \geq 2$ be even and let r be a non-zero integer. Write $\mathcal{A}_{k,r}$ for the set of integers $d \geq 2$ such that the equation*

$$x^k + (x+r)^k + \cdots + (x+(d-1)r)^k = y^n, \qquad x,\ y,\ n \in \mathbb{Z}, \qquad n \geq 2 \quad (11.6)$$

has a solution (x, y, n). Then $\mathcal{A}_{k,r}$ has natural density 0; by this we mean

$$\lim_{X\to\infty} \frac{\#\{d \in \mathcal{A}_{k,r} \ :\ d \leq X\}}{X} = 0.$$

Remark: If k is odd, then $\mathcal{A}_{k,r}$ contains all of the odd d: we can take $(x, y, n) = (r(1-d)/2, 0, n)$. Thus the conclusion of the theorem does not hold for odd k.

Chapter 12

Some Properties of Bernoulli Numbers and Polynomials

In our considerations of the case $k = 2$, we have already seen the degree 2 Bernoulli polynomial,

$$B_2(x) := x^2 - x + 1/6.$$

The even degree Bernoulli polynomials play a crucial role in our consecutive power sums. Therefore, in this section, we summarise some classical properties of Bernoulli numbers and polynomials. These are found in many references, including DLMF and [Cohen, 2007b, Chapter 9].

12.1 Background: Bernoulli Numbers and Polynomials

The **Bernoulli numbers** B_k are defined via the expansion

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

The first few Bernoulli numbers are

$$B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_3 = 0, \quad B_4 = -1/30, \quad B_5 = 0, \quad B_6 = 1/42.$$

It is easy to show that $B_{2k+1} = 0$ for all $k \geq 1$. The B_k are rational numbers, and the Von Staudt–Clausen theorem asserts for $k \geq 2$ an even integer,

$$B_k + \sum_{(p-1)|k} \frac{1}{p} \in \mathbb{Z}$$

where the sum ranges over primes p such that $(p-1) \mid k$.

The *k-th Bernoulli polynomial* can be defined by[1]:

$$B_k(x) = \sum_{m=0}^{k} \binom{k}{m} B_m x^{k-m}. \tag{12.1}$$

Thus it is a monic polynomial with rational coefficients, and all primes appearing in the denominators are bounded by $k+1$. It satisfies the symmetry

$$B_k(1-x) = (-1)^k B_k(x), \tag{12.2}$$

the identity

$$B_k(x+1) - B_k(x) = kx^{k-1}, \tag{12.3}$$

and the recurrence relation

$$B_k'(x) = kB_{k-1}(x). \tag{12.4}$$

Whilst all the above results have been known since at least the 19th century, we also make use of the following far more recent and difficult theorem due to Brillhart [1969] and Dilcher [2008].

Theorem 12.1.1 (Brillhart and Dilcher)**.** *The Bernoulli polynomials are squarefree.*

12.2 Application: Bernoulli Polynomials and Power Sums

Lemma 12.2.1. *Let r be a non-zero integer and k, $d \geq 1$. Then*

$$x^k + (x+r)^k + \cdots + (x+r(d-1))^k = \frac{r^k}{k+1}\left(B_{k+1}\left(\frac{x}{r}+d\right) - B_{k+1}\left(\frac{x}{r}\right)\right).$$

This formula can be found in [DLMF, Section 24.4], but is easily deduced from identity (12.3).

Lemma 12.2.2. *Let $q \geq k+3$ be a prime. Let a, r, d be integers with $d \geq 2$, and $r \neq 0$. Suppose $q \mid d$ and $q \nmid r$. Then*

$$a^k + (a+r)^k + \cdots + (a+r(d-1))^k \equiv r^k \cdot d \cdot B_k(a/r) \pmod{q^2}.$$

[1]Unfortunately, it is traditional to use the same notation for the Bernoulli numbers and the Bernoulli polynomials, denoting the former by B_k and the latter by $B_k(x)$.

Proof. By Taylor's Theorem

$$B_{k+1}(x+d) = B_{k+1}(x) + d \cdot B'_{k+1}(x) + \frac{d^2}{2} B^{(2)}_{k+1}(x) + \cdots + \frac{d^{k+2}}{(k+1)!} \cdot B^{(k+1)}_{k+1}(x).$$

It follows from the assumption $q \geq k+3$ that the coefficients of $B_{k+1}(x)$ are q-adic integers. Thus the coefficients of the polynomials $B^{(i)}_{k+1}(x)/i!$ are also q-adic integers. As $q \mid d$ and $q \nmid r$ we have

$$B_{k+1}\left(\frac{a}{r} + d\right) - B_{k+1}\left(\frac{a}{r}\right) \equiv d \cdot B'_{k+1}(a/r) \pmod{q^2}.$$

The lemma follows from identity (12.4) and Lemma 12.2.1. □

Lemma 12.2.3. *Let k and r be integers with $k \geq 2$ and $r \neq 0$. Let $q \geq k+3$ be a prime not dividing r such that the congruence $B_k(x) \equiv 0 \pmod{q}$ has no solutions. Let d be a positive integer such that $\operatorname{ord}_q(d) = 1$. Then equation (11.6) has no solutions (i.e. $d \notin \mathcal{A}_{k,r}$).*

Proof. Suppose $(x, y, n) = (a, b, n)$ is a solution to (11.6). By Lemma 12.2.2,

$$r^k \cdot d \cdot B_k(a/r) \equiv b^n \pmod{q^2}.$$

However, the hypotheses of the lemma ensure that the left-hand side has q-adic valuation 1. Thus $\operatorname{ord}_q(b^n) = 1$ giving a contradiction. □

Remarks:

- If we fix integers d and k, then Lemma 12.2.3 provides a criterion to "quickly" deduce[2] whether equation (11.6) has no solutions.
- For $k \geq 3$ odd, the k-th Bernoulli polynomial has known rational roots 0, 1/2, 1. Thus the criterion in the lemma fails to hold for all primes q.
- The second Bernoulli polynomial is $B_2(x) = x^2 - x + 1/6$. By quadratic reciprocity, this has a root modulo $q \nmid 6$ if and only if $q \equiv \pm 1 \pmod{12}$. We thus recover the result of Bai and Zhang mentioned in the introduction: if $q \equiv \pm 5 \pmod{12}$ and $\operatorname{ord}_q(d) = 1$ then (11.5) has no solutions with $k = 2$.

[2]The computation relies upon being able to compute the degree k Bernoulli polynomial modulo some prime q. Computational aspects for the Bernoulli numbers and polynomials have been extensively studied, and while in theory this computation can be done, in practice it can be difficult. While researching this problem, we were able to compute all Bernoulli polynomials modulo some prime of degree less than $70,000$. This was mainly thanks to the clever algorithm in Harvey [2010].

Chapter 13

A Galois Property of Even Degree Bernoulli Polynomials

In this chapter, we begin with a proposition that defines the "quadratic reciprocity equivalent" that we are searching for.

Proposition 13.0.1. *Let $k \geq 2$ be even, and let G_k be the Galois group of the Bernoulli polynomial $B_k(x)$. Then there is an element $\mu \in G_k$ that acts freely on the roots of $B_k(x)$.*

By *acting freely* on the roots, we mean that $\mu(\alpha) \neq \alpha$ for every root α of $B_k(x)$.

Proposition 13.0.1 asserts that this object, μ exists. Assuming the proposition, our density results then follow by applying Chebotarev's theorem and we will prove precisely this implication in this chapter (see Section 13.3 for a proof of Proposition 13.0.1 implies Theorem 11.2.1).

There is a long-standing conjecture that the even Bernoulli polynomials are irreducible; see for example Brillhart [1969], Carlitz [1952], Kimura [1988]. One can easily deduce Proposition 13.0.1 from this conjecture, however, we are able to give an unconditional proof of Proposition 13.0.1, see the final chapter, Chapter 15.

As noted previously, if k is odd, then $B_k(x)$ has rational roots 0, 1/2, 1, so the conclusion of the proposition certainly fails for odd k.

13.1 Background: Chebotarev Density Theorem

In this section, we state the Chebotarev Density Theorem which will be needed in proving Theorem 11.2.1.

First of all, we start by stating Chebotarev's Density Theorem. For this we we need some definitions. Let $\mathbb{P}$ be the set of primes, and let $\mathbb{P}'$ be a subset of $\mathbb{P}$. We define the *Dirichlet density* of $\mathbb{P}'$ to be the limit (if it exists)

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathbb{P}'} 1/p^s}{\sum_{p\in\mathbb{P}} 1/p^s}.$$

Since $\sum_{p\in\mathbb{P}} 1/p$ diverges, we see that if $\mathbb{P}'$ has positive Dirichlet density, then $\sum_{p\in\mathbb{P}'} 1/p$ also diverges.

As examples of sets of primes with positive Dirichlet density, we can now restate the theorem of Dirichlet in a stronger form (see, for example, [Murty, 2008, Section 2.3]).

Theorem 13.1.1 (Dirichlet)**.** *Let a and n be coprime integers with $n \geq 1$. Then the set of primes $p \equiv a \pmod{n}$ has Dirichlet density $1/\varphi(n)$, where φ is the Euler-totient function.*

Some Algebraic Number Theory

We need to also recall some facts from basic algebraic number theory. Let $K/\mathbb{Q}$ be a finite Galois extension and write $\mathcal{O}_K$ for the ring of integers of K. Let p be an unramified prime, and let $\mathfrak{P} \mid p$ be a prime ideal of $\mathcal{O}_K$. Associated to $\mathfrak{P}$ is the *Frobenius automorphism* $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$. This is the unique element of $\mathrm{Gal}(K/\mathbb{Q})$ satisfying

$$\mathrm{Frob}_{\mathfrak{P}}(a) \equiv a^p \pmod{\mathfrak{P}}$$

for all $a \in \mathcal{O}_K$. The assumption that p is unramified in K is needed to guarantee the uniqueness of $\mathrm{Frob}_{\mathfrak{P}}$. We point out that $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbb{Q}_p)$ is contained in $\mathrm{Gal}(K/\mathbb{Q})$ and is in fact generated by the Frobenius element $\mathrm{Frob}_{\mathfrak{P}}$.

If $\mathfrak{P}'$ is another prime of $\mathcal{O}_K$ above p then there is some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Observe that

$$\mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1}(a) \equiv (\sigma^{-1}(a))^p \pmod{\mathfrak{P}}$$

for all $a \in \mathcal{O}_K$. Applying σ to both sides gives

$$(\sigma\, \mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1})(a) \equiv a^p \pmod{\mathfrak{P}'}$$

since $\sigma(\mathfrak{P}) = \mathfrak{P}'$. It follows that $\sigma\, \mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1} = \mathrm{Frob}_{\mathfrak{P}'}$. Hence $\mathrm{Frob}_{\mathfrak{P}}$ and $\mathrm{Frob}_{\mathfrak{P}'}$ are conjugate. Now to an unramified prime p we associate a *Frobenius automorphism*

$\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$: we simply choose any $\mathfrak{P}$ and let Frob_p be $\mathrm{Frob}_{\mathfrak{P}}$. Thus Frob_p is really only defined up to conjugation.

Chebotarev Density Theorem

We are now ready to state the Chebotarev density theorem. Two excellent references for this are: [Murty and Esmonde, 2005, Chapter 11] and [Stevenhagen and Lenstra, 1996].

Theorem 13.1.2 (Chebotarev)**.** *Let $K/\mathbb{Q}$ be a finite Galois extension and write G for the Galois group. Let $C \subseteq G$ be a conjugacy class of elements in G. Then the set of unramified primes p with $\mathrm{Frob}_p \in C$ has Dirichlet density $\#C/\#G$.*

Before we give the proof that Proposition 13.0.1 implies Theorem 11.2.1, we state and prove a handful of useful lemmas.

Lemma 13.1.3. *Let $f \in \mathbb{Q}[x]$ be a polynomial with splitting field K. Let p be a prime satisfying the following conditions:*

(i) p is unramified in K;

(ii) p does not divide the denominator of any of the the coefficients of f;

(iii) p does not divide the numerator of the discriminant of f;

(iv) Frob_p acts freely on the roots of f.

Then the congruence $f(x) \equiv 0 \pmod{p}$ does not have any solutions.

Proof. Suppose $f(x) \equiv 0 \pmod{p}$ has a solution (for this to even make sense we need assumption (ii)). By Hensel's Lemma, which uses assumption (iii), this mod p root lifts to a root in $\mathbb{Q}_p$. Thus Frob_p fixes this root. This contradicts (iv). □

Lemma 13.1.4. *Let $f \in \mathbb{Q}[x]$ with splitting field K and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Suppose $\mu \in G$ acts freely on the roots of f. Then any μ' in the conjugacy class of μ also acts freely on the roots of f.*

Proof. Suppose μ, μ' are conjugate so we can write $\mu = \sigma^{-1}\mu'\sigma$ for some $\sigma \in G$. Suppose that μ' does not act freely on the roots. So there is a root $\alpha \in K$ fixed by μ'; i.e. $\mu'(\alpha) = \alpha$. But then $\beta = \sigma^{-1}(\alpha)$ is also a root of f and

$$\begin{aligned}\mu(\beta) &= \sigma^{-1}\mu'\sigma(\beta)\\ &= \sigma^{-1}\mu'(\alpha)\\ &= \sigma^{-1}(\alpha) = \beta.\end{aligned}$$

Thus μ fixes the root β. This contradicts the assumption that μ acts freely on the roots. $\square$

The following is a well-known corollary of the Chebotarev density theorem. See for example [Cassels and Fröhlich, 1967, Chapter VIII], but we give the proof.

Corollary 13.1.5. *Let $f \in \mathbb{Q}[x]$ have splitting field K and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Suppose there is an element $\mu \in G$ that acts freely on the roots of f. Then there is a subset of primes p of positive Dirichlet density such that the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions.*

Proof. Let C be the conjugacy class of μ. We know by Lemma 13.1.4 that every element of C acts freely on the roots of f. Now by the Chebotarev density theorem the set of primes p with $\mathrm{Frob}_p \in C$ has Dirichlet density $\#C/\#G$. In particular, this density is positive. We remove from this set without affecting the density the primes that divide the denominators of f, ramify in K or divide the numerator of the discriminant of f. Now if p is any prime belonging to this set then by Lemma 13.1.3 the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions. $\square$

13.2 Background: Niven's Theorem

Let $\mathcal{A}$ be a set of positive integers. For X positive, define

$$\mathcal{A}(X) = \#\{d \in \mathcal{A} : d \leq X\}.$$

The **natural density** of $\mathcal{A}$ is defined as the limit (if it exists)

$$\delta(\mathcal{A}) = \lim_{X \to \infty} \frac{\mathcal{A}(X)}{X}.$$

For a given prime q, define

$$\mathcal{A}^{(q)} = \{d \in \mathcal{A} \ : \ \mathrm{ord}_q(d) = 1\}.$$

We shall need the following result of [Niven, 1951, Corollary 1].

Theorem 13.2.1 (Niven)**.** *Let $\{q_i\}$ be a set of primes such that $\delta(\mathcal{A}^{(q_i)}) = 0$ and $\sum q_i^{-1} = \infty$. Then $\delta(\mathcal{A}) = 0$.*

As noted previously if $\{q_i\}$ is a set of positive Dirichlet density then $\sum q_i^{-1} = \infty$.

13.3 Proposition 13.0.1 implies Theorem 11.2.1

We now suppose Proposition 13.0.1 and use it to deduce Theorem 11.2.1. Let $k \geq 2$ be an even integer. Write G_k for the Galois group of the Bernoulli polynomial $B_k(x)$. Let $\mu \in G_k$ be the element acting freely on the roots of $B_k(x)$ whose existence is asserted by Proposition 13.0.1. By Corollary 13.1.5 there is a set of primes $\{q_i\}_{i=1}^{\infty}$ having positive Dirichlet density such that the congruence $B_k(x) \equiv 0 \pmod{q}$ has no solutions for $q = q_i$. We omit from $\{q_i\}$ (without affecting the density) the following:

- primes $q \leq k + 2$;
- primes q dividing r;
- primes q dividing the numerator of the discriminant of $B_k(x)$ (which is non-zero by Theorem 12.1.1).

Now let $\mathcal{A} = \mathcal{A}_{k,r}$ be as in the statement of Theorem 11.2.1. By Lemma 12.2.3, if $\mathrm{ord}_{q_i}(d) = 1$ then $d \notin \mathcal{A}$. It follows that $\mathcal{A}^{(q_i)} = \emptyset$. By Theorem 13.2.1, we have $\delta(\mathcal{A}) = 0$ as required.

Sometimes you can try too hard,
just relax and let it happen.

Winnie the Pooh, A. A. Milne

Chapter 14

A Picture is Worth a Thousand Math Symbols!

In this chapter, we first begin by giving a brief introduction to *Newton polygons* as they are a vital tool for us when proving Proposition 13.0.1. Along the way, we prove the following theorem:

Theorem 14.0.1 (Patel and Siksek [2017])**.** *Let k be even. Then $B_k(x)$ has no roots in $\mathbb{Q}_2$.*

This theorem is not essential in proving Proposition 13.0.1, however, its proof motivates the proof for the proposition.

14.1 Background: Local Fields, Newton Polygons

In this section, we aim to give a brief introduction to Newton Polygons. Primarily, we follow Gouvêa [1993] (Chapter 6, Section 4, pages 212–233). Another good reference for this is Cassels [1986].[1]

So lets begin drawing pictures of Newton polygons and analyzing the pictures. These pictures are really worth a thousand math symbols - if not more! The information we can gleam off of them is invaluable, and we shall be using the diagrams to extract valuable data in our consecutive like powers saga.

As an introductory example, let's choose one of the Bernoulli Polynomials; $B_6(x)$ for example:

$$B_6(x) := x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}.$$

[1] A personal favourite of mine as this was my very first book on number theory that I read many many moons ago. Plus I love the rustic feeling when flicking through pages of classic typewriter font!

Steps to draw a Newton Polygon

- Let p be a prime and choose a polynomial f with coefficients in $\mathbb{Q}_p$.
- Label the coefficients of the polynomial as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

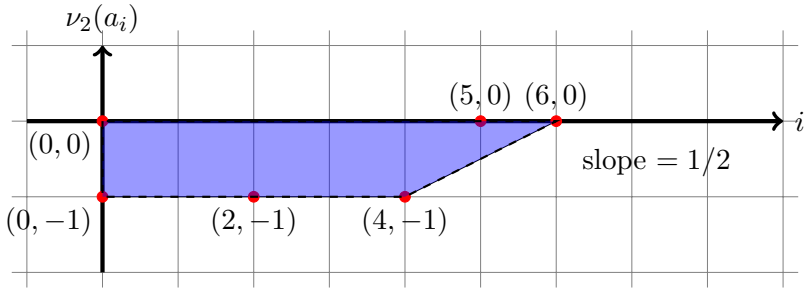
- On the Cartesian plane, draw the points $(i, \mathrm{ord}_p(a_i))$ for $0 \leq i \leq n$.
- The Newton polygon is the *convex hull of these points*. We draw this by taking the first point and placing our pen(cil) on that point facing down. Then rotate the pen anti-clockwise until we hit the next point. These two points are joined with a line, and we continue to rotate our pen(cil) anti-clockwise and draw lines until we have ran out of points.

Remark: If the first point is $(0, +\infty)$ then the convention is to usually ignore this point, and start with the next one. Encountering points which look like $(i, +\infty)$ can be ignored. The can be seen as being infinitely high on the piece of paper, and on rotating the pen(cil) anti-clockwise, we will never ever reach them. Ever.

Practise makes perfect!

Let's draw the Newton polygon for $B_6(x)$ at the prime 2. The points we need are

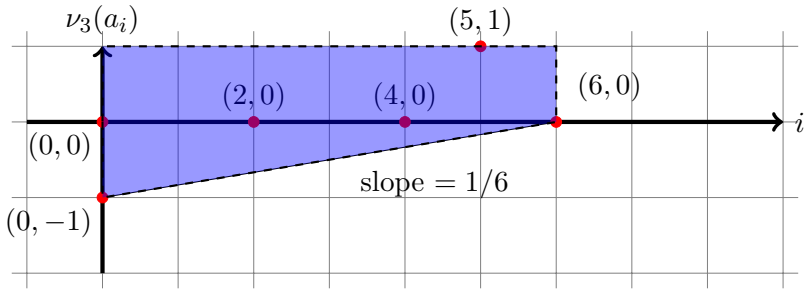
$$(0,-1), (1,+\infty), (2,-1), (3,+\infty), (4,-1), (5,0), (6,0).^2$$



[2]The diagram does not show the points $(i, +\infty)$. (Obviously!)

Let's draw the Newton polygon for $B_6(x)$ at the prime 3. The points we need are

$$(0,-1),(1,+\infty),(2,0),(3,+\infty),(4,0),(5,1),(6,0).^{3}$$



Now that we have acquired a new gadget, we can begin to explore further and make mathemagical[4] deductions from the Newton polygon.

One may see that the Newton polygon consists of *Line Segments* or portions of straight lines. Each segment of the Newton Polygon has very valuable information.

- Let's define a segment by the endpoints, i.e. S is the segment between the points (x_1, y_1) and (x_2, y_2).
- The *slope* of a segment is defined in the usual way as $(y_2 - y_1)/(x_2 - x_1)$[5].
- The *length* of a segment, is defined as the *projective length*. This is much simpler than it sounds: it is $x_2 - x_1$. You can think of it as projecting the line segment onto the x-axis.

Very Useful Remarks: Each segment of the Newton polygon of f corresponds to a factor of f over $\mathbb{Q}_p$. Let l be the length and m be the slope of a segment. Then l is the degree of the corresponding factor, and the valuation of its roots (which belong to $\overline{\mathbb{Q}_p}$) is $-m$. If the segment does not pass through any lattice points (apart from its end points), then the corresponding polynomial is irreducible. In particular, if a segment has non-integral slope, then we know that the roots of the corresponding polynomial do not belong to $\mathbb{Q}_p$.

[3]Neither do they [the points $(i, +\infty)$] show in the diagram for the 3-adic Newton Polygon, and any further Newton polygons which appear in this thesis.

[4]Not a typo. The Newton polygon really does feel magical! 🪄

[5]This is probably looking very familiar - you would have most likely encountered it in high-school, finding equations of straight lines, the gradient, derivatives... Apologies if I have awoken some deeply repressed ghosts of calculus within!

Using the analysis above, we can deduce the following information about $B_6(x)$ using the 2-adic and 3-adic Newton polygons.

- At the prime 2, the Newton polygon for $B_6(x)$ has exactly two segments: the first horizontal piece of length 4 and the second of length 2 and slope 1/2. Thus, $B_6(x) = f_1(x)f_2(x)$ where f_1 and f_2 are polynomials defined over $\mathbb{Q}_2$ of degree respectively 4 and 2. Notice that the first segment passes through the lattice points $(1,-1)$, $(2,-1)$, $(3,-1)$ so we cannot deduce from the Newton polygon that f_1 is irreducible. However, the second segment does not pass through any lattice points so f_2 is irreducible. Moreover, the 4 roots of f_1 have valuation 0 and the 2 roots of f_2 have valuation $-1/2$. In particular, we can deduce that $B_6(x)$ has at most 4 roots in $\mathbb{Q}_2$, and that these all have valuation 0 so they belong to $\mathbb{Z}_2$.

- From the Newton polygon for $B_6(x)$ at the prime 3, we see immediately that $B_6(x)$ is irreducible over $\mathbb{Q}_3$. Moreover, its 6 roots (none of which are in $\mathbb{Q}_3$) all have valuation $-1/6$. Mathemagical!

14.2 Application: Two is the Oddest Prime

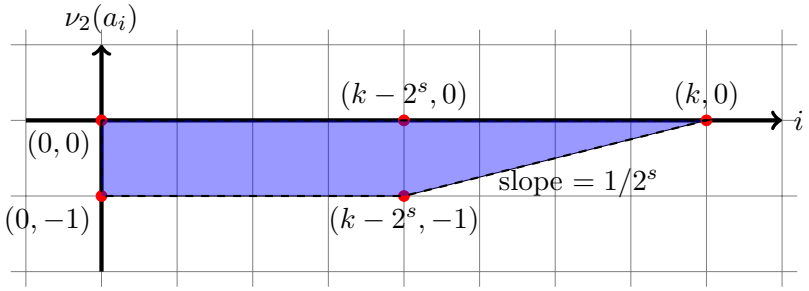
In this section, we examine the the 2-adic Newton polygon of any even degree Bernoulli polynomial. Through the study of the 2-adic Newton polygon, we prove the following theorem:

Theorem 14.2.1 (Patel and Siksek [2017])**.** *Let k be even. Then $B_k(x)$ has no roots in $\mathbb{Q}_2$.*

Remark: Inkeri [1959] showed that $B_k(x)$ has no rational roots for k a positive even integer. His proof required very precise (and difficult) estimates for the real roots of $B_k(x)$. Considerations of the 2-adic Newton polygon for the Bernoulli polynomials (see Lemma 14.2.2 below) allows us to give a much simpler proof of a stronger result.

The Newton Polygon: of $B_k(x)$ for $k = 2^s \cdot t$, $s \geq 1$.

$$B_k(x) = \sum_{i=0}^{k} \binom{k}{k-i} B_{k-i} x^i = \sum_{i=0}^{k} a_i x^i.$$



Lemma 14.2.2. *Let $k \geq 2$ be even and write $k = 2^s t$ where t is odd and $s \geq 1$. The 2-adic Newton polygon of $B_k(x)$ consists two segments:*

(i) a horizontal segment joining the points $(0,-1)$ and $(k-2^s,-1)$;

(ii) a segment joining the points $(k-2^s,-1)$ and $(k,0)$ of slope $1/2^s$.

Proof. Consider the definition of $B_k(x)$ in (12.1). We know that $B_0 = 1$, $B_1 = -1/2$ and $B_m = 0$ for all odd $m \geq 3$. From the Von Staudt–Clausen theorem, we know that $\mathrm{ord}_2(B_m) = -1$ for even $m \geq 2$. It follows that the Newton polygon is bounded below by the horizontal line $y = -1$.

We shall need to make use of the following result of Kummer (see Granville [1997]): if p is a prime, and u, v are positive integers then

$$\binom{u}{v} \equiv \binom{u_0}{v_0}\binom{u_1}{v_1} \pmod{p},$$

where u_0, u_1 are respectively the remainder and quotient on dividing u by p, and likewise v_0, v_1 are respectively the remainder and quotient on dividing v by p. Here we adopt the convention $\binom{r}{s} = 0$ if $r < s$. Applying this with $p = 2$ we see that

$$\binom{k}{2^s} = \binom{2^s t}{2^s} \equiv \binom{t}{1} \equiv t \equiv 1 \pmod{2}.$$

Thus the coefficient of x^{k-2^s} in $B_k(x)$ has 2-adic valuation -1. Since the constant coefficient of $B_k(x)$ also has valuation -1, we obtain the segment (i) as part of the Newton polygon. We also see that for $0 < v < 2^s$,

$$\binom{k}{v} \equiv 0 \pmod{2},$$

and so the valuation of the coefficient of x^{k-v} is ≥ 0. Finally the coefficient of x^k is $B_0 = 1$ and so has valuation 0. This gives segment (ii) and completes the proof. □

Proof of Theorem 14.2.1

Proof. Indeed, suppose $\alpha \in \mathbb{Q}_2$ is a root of $B_k(x)$. From the slopes of the Newton polygon segments we see that $\mathrm{ord}_2(\alpha) = 0$ or $-1/2^s$. As ord_2 takes only integer values on $\mathbb{Q}_2$, we see that $\mathrm{ord}_2(\alpha) = 0$ and so $\alpha \in \mathbb{Z}_2$. Let $f(x) = 2B_k(x) \in \mathbb{Z}_2[x]$. Thus $f(\alpha) = 0$ and so $f(\overline{\alpha}) = \overline{0} \in \mathbb{F}_2$. However, $\overline{\alpha} \in \mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. Now $f(\overline{0}) = \overline{(2B_k)} = \overline{1}$, and from (12.2) we know that $f(\overline{1}) = f(\overline{0}) = \overline{1}$. This gives a contradiction. □

Remark: Although Theorem 14.2.1 is not needed by us, its proof helps motivate part of the proof of Proposition 13.0.1.

People say nothing is impossible,
but I do nothing every day.

Winnie the Pooh, A. A. Milne

Chapter 15

Completing the Proof of Theorem 11.2.1

To complete the proof of Proposition 13.0.1, hence the proof of Theorem 11.2.1, we need to appeal to a little group theory. In this chapter, we begin with a section to outline the necessary preliminaries, with the final section bringing all the pieces together to finish the proof of Theorem 11.2.1.

15.1 Finding μ (via a Little Group Theory)

We shall need some definitions. Let H be a group acting on a set S. We say that the action is *transitive* if for every s, $t \in S$, there is some $\sigma \in H$ such that $\sigma(s) = t$. By the *Stabilizer* of an element $s \in S$ we mean the subgroup

$$\mathrm{Stab}(H, s) = \{\tau \in H \ : \ \tau(s) = s\}.$$

We make use of the following well-known fact.

Lemma 15.1.1. *If H acts transitively on S then any two stabilizers are conjugate.*

Proof. Let s, $t \in S$. As H is acting transitively there is some $\sigma \in H$ such that $\sigma(s) = t$. Now note that

$$\begin{aligned}
\tau \in \mathrm{Stab}(H, s) &\iff \tau(s) = s \\
&\iff \tau\sigma^{-1}\sigma(s) = s \\
&\iff \tau\sigma^{-1}(t) = s \\
&\iff \sigma\tau\sigma^{-1}(t) = \sigma(s) \\
&\iff \sigma\tau\sigma^{-1}(t) = t \\
&\iff \sigma\tau\sigma^{-1} \in \mathrm{Stab}(H, t).
\end{aligned}$$

Thus $\sigma \operatorname{Stab}(H, s)\sigma^{-1} = \operatorname{Stab}(H, t)$. □

Lemma 15.1.2. *Let $\pi : H \to C$ be a homomorphism for a group H to an abelian group C. Let H_1, H_2 be two subgroups of H that are conjugate. Then $\pi(H_1) = \pi(H_2)$.*

Proof. Suppose $\sigma H_1 \sigma^{-1} = H_2$. Let $h_2 \in H_2$. Then $h_2 = \sigma h_1 \sigma^{-1}$ for some $h_1 \in H_1$. Therefore $\pi(h_2) = \pi(\sigma)\pi(h_1)\pi(\sigma)^{-1}$. Now as C is abelian we may rewrite this as $\pi(h_2) = \pi(\sigma)\pi(\sigma)^{-1}\pi(h_1) = \pi(h_1)$. This proves the lemma. □

Lemma 15.1.3. *Let H be a finite group acting transitively on a finite set $\{\beta_1, \ldots, \beta_n\}$. Let $H_i \subseteq H$ be the stabilizer of β_i, and suppose $H_1 = H_2$. Let $\pi : H \to C$ be a surjective homomorphism from H onto a cyclic group C. Then there is some $\mu \in H$ acting freely on $\{\beta_1, \ldots, \beta_n\}$ such that $\pi(\mu)$ is a generator of C.*

Proof. Note that $\mu \in H$ acting freely on $\{\beta_1, \ldots, \beta_n\}$ is equivalent to μ not belonging to any of the stabilizers $H_1, \ldots, H_n$.

Let $m = \#C$ and write $C = \langle \sigma \rangle$. Consider the subset

$$C' = \{\sigma^r \ : \ \gcd(r, m) = 1\};$$

this is the set of elements that are cyclic generators of C. Thus the lemma asserts the existence of μ such that

$$\pi(\mu) \in C', \qquad \mu \notin \bigcup_{i=1}^{n} H_i.$$

If the conclusion of the lemma is false then

$$\pi^{-1}(C') \subseteq \bigcup_{i=1}^{n} H_i.$$

Suppose this is the case and we aim for a contradiction. Then we immediately see that

$$\pi^{-1}(C') = \bigcup_{i=1}^{n} \pi^{-1}(C') \cap H_i.$$

However, according to the hypotheses of the lemma, $H_1 = H_2$. Thus we may rewrite this as

$$\pi^{-1}(C') = \bigcup_{i=2}^{n} \pi^{-1}(C') \cap H_i.$$

In particular,

$$\#\pi^{-1}(C') \leq \sum_{i=2}^{n} \#\pi^{-1}(C') \cap H_i. \tag{15.1}$$

The set C' has cardinality $\varphi(m)$, where φ is the Euler totient function. As π is surjective we see that

$$\#\pi^{-1}(C') = \frac{\varphi(m)}{m} \cdot \#H. \tag{15.2}$$

As H acts transitively on the β_i, the stabilizers H_i are conjugate by Lemma 15.1.1 and so have the same image $\pi(H_i)$ in C by Lemma 15.1.2. If this image is a proper subgroup of C, then take μ to be any preimage of σ. Thus $\pi(\mu) = \sigma$ is a generator of C, and moreover, μ does not belong to any of the stabilizers H_i and so acts freely on $\{\beta_1, \ldots, \beta_n\}$, completing the proof in this case. Thus we suppose that $\pi(H_i) = C$ for all i. It follows that

$$\#\pi^{-1}(C') \cap H_i = \frac{\varphi(m)}{m} \cdot \#H_i = \frac{\varphi(m)}{m} \cdot \frac{\#H}{n}, \tag{15.3}$$

where the second equality follows from the Orbit-Stabilizer Theorem. Finally we substitute (15.2) and (15.3) in (15.1) obtaining

$$\frac{\varphi(m)}{m} \cdot \#H \leq \frac{(n-1)}{n} \cdot \frac{\varphi(m)}{m} \cdot \#H$$

which gives the required contradiction.

□

15.2 Unconditional Proof of Proposition 13.0.1

We now complete the proof of Theorem 11.2.1 by proving Proposition 13.0.1. Fix an even $k \geq 2$, and let L be the splitting field of $B_k(x)$. Let $G_k = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(B_k(x))$ be the Galois group of $B_k(x)$. Let $\mathfrak{P}$ be a prime of L above 2. The 2-adic valuation ord_2 on $\mathbb{Q}_2$ has a unique extension to $L_{\mathfrak{P}}$ which we continue to denote by ord_2. We let $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subseteq G_k$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

From Lemma 14.2.2 we see that $B_k(x)$ factors as $B_k(x) = g(x)h(x)$ over $\mathbb{Q}_2$ where the factors g, h correspond respectively to the segments (i), (ii) in the lemma. Thus g, h have degree $k - 2^s$ and 2^s respectively. We denote the roots of g by $\{\alpha_1, \ldots, \alpha_{k-2^s}\} \subset L_{\mathfrak{P}}$ and the roots of h by $\{\beta_1, \ldots, \beta_{2^s}\} \subset L_{\mathfrak{P}}$. From the slopes of the segments we see that $\mathrm{ord}_2(\alpha_i) = 0$ and $\mathrm{ord}_2(\beta_j) = -1/2^s$. It clearly follows

that h is irreducible and therefore that H acts transitively on the β_j. Moreover, from the symmetry (12.2) we see that $1-\beta_1$ is a root of $B_k(x)$, and by appropriate relabelling we can suppose that $\beta_2 = 1-\beta_1$. In the notation of Lemma 15.1.3, we have $H_1 = H_2$. Now let $C = \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2)$, where $\mathbb{F}_{\mathfrak{P}}$ is the residue field of $\mathfrak{P}$. This group is cyclic generated by the Frobenius map: $\overline{\gamma} \mapsto \overline{\gamma}^2$. We let $\pi : H \to C$ be the induced surjection. By Lemma 15.1.3 there is some $\mu \in H$ that acts freely on the β_i and such that $\pi(\mu)$ generates C. To complete the proof of Proposition 13.0.1 it is enough to show that μ also acts freely on the α_i. Suppose otherwise, and let α be one of the α_i that is fixed by μ. As $\mathrm{ord}_2(\alpha) = 0$, we can write $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ for the reduction of α modulo $\mathfrak{P}$. Now α is fixed by μ, and so $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}$ is fixed by $\langle \pi(\mu) \rangle = C$. Thus $\overline{\alpha} \in \mathbb{F}_2$ and so $\overline{\alpha} = \overline{0}$ or $\overline{1}$. Now let $f(x) = 2B_k(x) \in \mathbb{Z}_2[x]$. Thus $f(\overline{\alpha}) = \overline{0}$. But $f(\overline{0}) = \overline{(2B_k)} = \overline{1}$, and from (12.2) we know that $f(\overline{1}) = f(\overline{0}) = \overline{1}$. This contradiction completes the proof.

Goodbye ..? Oh no, please. Can't we go back to page one and do it all over again?

— *Winnie the Pooh, A. A. Milne*

Bibliography

A. Baker. *Transcendental number theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1990.

M. A. Bennett, V. Patel, and S. Siksek. Perfect powers that are sums of consecutive cubes. *Mathematika*, 63(1):230–249, 2017.

W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

J. Brillhart. On the Euler and Bernoulli polynomials. *J. Reine Angew. Math.*, 234: 45–64, 1969.

Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

L. Carlitz. Note on irreducibility of the Bernoulli and Euler polynomials. *Duke Math. J.*, 19:475–481, 1952.

J. W. S. Cassels. A Diophantine equation. *Glasgow Math. J.*, 27:11–18, 1985.

J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

J. W. S. Cassels and A. Fröhlich. *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical

Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007a.

H. Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007b.

A. Del Centina. Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's last theorem. *Arch. Hist. Exact Sci.*, 62(4):349–392, 2008.

F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. ISBN 0-387-23229-X.

L. E. Dickson. History of the theory of numbers, vol. ii, chelsea publ. *Co., New York*, 1971.

K. Dilcher. On multiple zeros of Bernoulli polynomials. *Acta Arith.*, 134(2):149–155, 2008.

DLMF. NIST Digital Library of Mathematical Functions. http://dlmf.nist.gov/24, Release 1.0.11 of 2016-06-08, 2016. URL `http://dlmf.nist.gov/24`. Online companion to Olver et al. [2010].

L. Euler. *Vollständige Anleitung zur Algebra*, volume 2. St. Petersburg, 1770.

F. Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, 1993. An introduction.

A. Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997.

D. Harvey. A multimodular algorithm for computing Bernoulli numbers. *Math. Comp.*, 79(272):2361–2370, 2010.

K. Inkeri. The real roots of Bernoulli polynomials. *Ann. Univ. Turku. Ser. A I*, 37: 20, 1959.

N. Kimura. On the degree of an irreducible factor of the Bernoulli polynomials. *Acta Arith.*, 50(3):243–249, 1988.

A. Kraus. Majorations effectives pour l'équation de Fermat généralisée. *Canad. J. Math.*, 49(6):1139–1161, 1997.

M. Laurent. Linear forms in two logarithms and interpolation determinants. II. *Acta Arith.*, 133(4):325–348, 2008.

E. Lucas. *Recherches sur l'analyse indéterminée et l'Arithmétique de Diophante*. Préface de J. Itard. Librairie Scientifique et Technique Albert Blanchard, Paris, 1961.

M. R. Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

M. R. Murty and J. Esmonde. *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2005.

T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk Mat. Forenings Skr.*, 1(2):14 pages, 1921.

I. Niven. The asymptotic density of sequences. *Bull. Amer. Math. Soc.*, 57:420–434, 1951.

F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, editors. *NIST Handbook of Mathematical Functions*. Cambridge University Press, New York, NY, 2010. Print companion to DLMF.

C. Pagliani. Solution du problème d'analyse indéterminée énoncé à la pag. 212 du présent volume. *Ann. Math. Pures Appl. [Ann. Gergonne]*, 20:382–384, 1829/30.

V. Patel and S. Siksek. On powers that are sums of consecutive like powers. *Res. Number Theory*, 3:Art. 2, 7, 2017.

K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

S. Siksek. The modular approach to Diophantine equations. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 151–179. Soc. Math. France, Paris, 2012.

J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

I. Stewart and D. Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.

R. J. Stroeker. On the sum of consecutive cubes being a perfect square. *Compositio Math.*, 97(1-2):295–307, 1995. Special issue in honour of Frans Oort.

S. Uchiyama. On a Diophantine equation. *Proc. Japan Acad. Ser. A Math. Sci.*, 55 (9):367–369, 1979.

A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Z. Zhang. On the Diophantine equation $(x-1)^k + x^k + (x+1)^k = y^n$. *Publ. Math. Debrecen*, 85(1-2):93–100, 2014.

Z. Zhang and M. Bai. On the Diophantine equation $(x+1)^2+(x+2)^2+\cdots+(x+d)^2 = y^n$. *Funct. Approx. Comment. Math.*, 49(1):73–77, 2013.